

明 細 書

受信装置、送出装置、セキュリティモジュール、及びデジタル権利管理システム

技術分野

[0001] 本発明は、デジタル放送、インターネットなどで配信される映像、音楽などのデジタルコンテンツの利用権利を管理し、ユーザが利用権利に基づき端末装置でデジタルコンテンツを利用するシステムに関し、特に、端末装置におけるデジタルコンテンツの利用権利の取得を、事業者の意図に従って確実に制御することが可能なシステムに関する。

背景技術

[0002] 近年、音楽、映像などのデジタルコンテンツ(以下、コンテンツと記述)を、デジタル放送、デジタルCATV(Cable Television)、インターネットなどを通じて、放送局から端末装置に配信し、端末装置においてコンテンツを利用することが可能なコンテンツ配信サービスが実用化の段階を迎えている。このコンテンツ配信サービスでは、コンテンツの著作権を保護し、悪意あるユーザなどによるコンテンツの不正利用を防止するため、著作権保護技術が用いられるのが一般的である。著作権保護技術とは、具体的には、暗号技術や認証技術などを用いて、ユーザがコンテンツを再生したり、記録メディアにコピーしたりといったようなコンテンツの利用を、セキュアに制御する技術である。著作権保護技術を用いることにより、放送局などのコンテンツプロバイダ、サービスプロバイダが、端末装置におけるユーザのコンテンツ利用をセキュアに制御することが可能となる。

[0003] ところで、近年、HDD(Hard Disk Drive)などの大容量蓄積手段を有する端末装置において、配信されたコンテンツを一旦端末装置に蓄積し、ユーザが好きなときに蓄積されたコンテンツを視聴するという、ユーザ利便性の高い利用形態が検討されている。日本におけるデジタル放送の規格化団体であるARIB(Association of Radio Industries and Businesses)においては、大容量蓄積機能を活用するデジタル放送方式として、サーバ型放送方式が規格化されており、特にコンテンツの蓄

積時における再生を限定するため方式として、限定再生方式が策定されている。なお、サーバ型放送方式における限定再生方式については、ARIB STD-B25 4.1版が詳しい。

- [0004] このような蓄積機能を有する端末装置においては、コンテンツとともに、コンテンツの利用権利であるライセンスも端末装置に蓄積されるため、ライセンスを自由に複製することが可能である。その結果、同一のコンテンツについて複数のライセンスが無制限に取得できてしまう可能性が生ずる。もちろん、通常ライセンスは暗号化が施された状態で配信されるため、どのユーザであっても自由に利用できるわけではないが、少なくとも放送局との視聴契約を行ったユーザについては、特に月ぎめ契約(サブスクリプション)の場合などは、ライセンスを無制限に取得することが容易に可能となる。
- [0005] このような課題と類似の課題を解決するデジタル権利管理システムとして、記録媒体に書き出すコンテンツの数を制限するため、記録媒体に書き出すコンテンツIDをリストで管理する手法が開示されている(例えば、特許文献1参照)。この手法においては、コンテンツIDを記載したリストサイズの無制限な増加を防止するため、リストサイズの上限も管理しており、リストのサイズが上限に達した場合には、リストへの登録日時の古いレコードの順にコンテンツIDを削除するようになっている。
- 特許文献1:特開2004-5526号公報
- 発明の開示
- 発明が解決しようとする課題
- [0006] しかしながら、従来のデジタル権利管理システムでは、登録日時の古い順に、リストからレコードを削除する方式であるので、リストへのライセンスIDの登録・削除の繰り返しにより、結果的に複数の同一ライセンスを無制限に不正に取得されてしまう可能性があり、ユーザの取得可能なライセンス数を制限したいという事業者の権利を十分に保護することができない、という課題がある。
- [0007] また、ライセンスの管理をICカード等を用いておこなう場合、ユーザが実際にコンテンツを視聴するか否かに関わらず、取得したライセンスを全てICカードに取り込む管理方法では、ICカードの容量を圧迫してしまうという問題がある。

[0008] 本発明は、こうした従来の問題点を解決するものであり、デジタル放送などにおいてライセンスを配信する場合に、ユーザによる無制限なライセンス取得を防止するとともに、ICカード等に記録されるライセンス管理に関する情報のサイズの増大を防止することが可能な受信装置及び送出装置を提供することを目的としている。

課題を解決するための手段

[0009] 上記目的を達成するために、本発明に関わる受信装置は、コンテンツの利用許諾を与えるためのライセンスを配信する送出装置から、前記ライセンスを取得し、当該ライセンスに基づき前記コンテンツを利用する受信装置であって、前記ライセンスには、少なくとも前記ライセンスを前記受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限及びライセンスIDが付与され、前記受信装置は、前記送出装置から送出される前記ライセンスを取り込むライセンス取り込み手段と、少なくとも前記ライセンス取り込み期限まで、前記ライセンスIDと前記ライセンス取り込み期限とを含むライセンス取り込み履歴を記録する履歴記録手段と、前記ライセンス取り込み手段において取り込んだライセンスのライセンスIDと同一のライセンスIDが前記ライセンス取り込み履歴に存在する場合に、前記ライセンス取り込み手段における当該ライセンスの取り込みを抑制するライセンス取り込み抑制手段とを備えることを特徴とする。

[0010] この構成により、受信装置のライセンス取り込み抑制手段は、ライセンスIDとライセンス取り込み期限とを用いて、ライセンスの不正取得を防止することが可能となる。

[0011] また、本発明に係る受信装置は、さらに、前記ライセンス取り込み手段で取り込む前の暗号化ライセンスを一旦復号して、復号済みライセンスを生成するライセンス復号手段と、前記暗号化ライセンスの暗号化に用いた暗号鍵とは異なる暗号鍵を用いて、前記復号済みライセンスを再暗号化して再暗号化ライセンスを生成する再暗号化手段と、少なくとも前記再暗号化ライセンスを蓄積する蓄積手段とを備えることを特徴とする。

[0012] さらに、本発明に係る受信装置においては、前記ライセンスには、さらに、前記再暗号化手段における再暗号化が可能な期限である暗号変換期限が付加され、前記再暗号化手段は、前記暗号変換期限内のライセンスに対して再暗号化を行って前記

再暗号化ライセンスを生成し、前記再暗号化ライセンスを前記蓄積手段に蓄積することを特徴とする。

- [0013] これらの構成により、暗号変換期限を用いて正規のライセンスに対してマーキングを行うと共に、再暗号化手段における再暗号化後のライセンスを蓄積手段に蓄積しておくことができるために、ユーザが正規に使用するライセンスのみをICカード等に取り込んで、ライセンスに関する情報でICカードの容量が圧迫されるという問題を解決することが可能となる。
- [0014] また、本発明に係る送出装置は、コンテンツの利用許諾を与えるためのライセンスに基づきコンテンツを利用する受信装置に対して前記ライセンスを送出する送出装置であって、前記ライセンスを生成するライセンス生成手段と、前記ライセンスに、識別番号であるライセンスIDを付与するライセンスID付与手段と、前記ライセンスに、前記受信装置において、少なくとも当該ライセンスを当該受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限を付与するライセンス取り込み期限付与手段と、少なくとも前記ライセンスID、前記ライセンス取り込み期限が付与された前記ライセンスを、前記受信装置に送出する送出手段とを備えることを特徴とする。
- [0015] この構成により、送出装置においては、ライセンスに少なくともライセンスID及びライセンス取り込み期限を付与して受信装置側に送出することが可能となり、ライセンスに関する情報管理をより適切に行うことが可能となる。
- [0016] また、本発明に係る送出装置において、前記受信装置は、前記ライセンスの暗号化に用いた暗号鍵とは異なる暗号鍵を用いて、前記復号済みライセンスを再暗号化して再暗号化ライセンスを生成する再暗号化手段を備え、前記送出装置は、さらに、前記ライセンスに、前記再暗号化手段における再暗号化が可能な期限である暗号変換期限を付加する暗号変換期限付与手段を備え、前記送出手段は、少なくとも前記ライセンスID、前記暗号変換期限が付与されたライセンスを、前記受信装置に送出することを特徴とする。
- [0017] この構成により、送出装置側で、受信装置において再暗号化の判断情報となる暗号変換期限をライセンスに付与して、受信装置側に送信することが可能となる。

[0018] また、本発明に係るセキュリティモジュールは、ライセンスに基づきコンテンツを利用する端末装置と連携して動作するセキュリティモジュールであって、前記ライセンスには、少なくとも前記ライセンスを前記受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限及びライセンスIDが付与され、前記セキュリティモジュールは、前記送出装置から送出される前記ライセンスを取り込むライセンス取り込み手段と、少なくとも前記ライセンス取り込み期限まで、前記ライセンスIDと前記ライセンス取り込み期限とを含むライセンス取り込み履歴を記録する履歴記録手段と、前記ライセンス取り込み手段において取り込んだライセンスのライセンスIDと同一のライセンスIDが前記ライセンス取り込み履歴に存在する場合に、前記ライセンス取り込み手段における当該ライセンスの取り込みを抑制するライセンス取り込み抑制手段とを備えることを特徴とする。

[0019] さらに、本発明に係るセキュリティモジュールは、さらに、前記ライセンス取り込み手段で取り込む前の暗号化ライセンスを一旦復号して、復号済みライセンスを生成するライセンス復号手段と、前記暗号化ライセンスの暗号化に用いた暗号鍵とは異なる暗号鍵を用いて、前記復号済みライセンスを再暗号化して再暗号化ライセンスを生成する再暗号化手段とを備えることを特徴とする。

[0020] これらの構成により、セキュリティモジュールにおいて、ライセンスに付与されているライセンス取り込み期限や暗号変換期限の情報を用いて、ライセンスが不正に使用されることや、ライセンス管理における情報がセキュリティモジュールの容量を圧迫するという問題を解決することが可能となる。

[0021] 尚、前記目的を達成するために、本発明は、前記受信装置、前記送出装置及び前記セキュリティモジュールの特徴的な構成手段をステップとする受信方法、送出方法及びライセンス取得方法としたり、それらのステップを全て含むプログラムとして実現することもできる。そして、そのプログラムは、受信装置及び送出装置が備えるROM等に格納しておくだけでなく、CD-ROM等の記録媒体や通信ネットワークを介して流通させることもできる。

発明の効果

[0022] 本発明によれば、端末装置で取得したライセンスのIDと有効期限とを、ライセンス

の取得履歴として管理し、少なくともライセンスの取り込み期限までライセンス取得履歴を保持しておくことにより、無制限なライセンス取得の防止と、管理するデータサイズの増大の防止とを両立することが可能となる。また、暗号変換期限を用いることにより、ユーザが実際に使用するライセンスのみをICカードに取り込むことができ、ICカードに記録されるデータ容量を適切に管理できる。

図面の簡単な説明

[0023] [図1]図1は、本発明の実施の形態に係るコンテンツ配信システムの全体の概略構成を示す図である。

[図2]図2は、本発明の実施の形態に係る暗号スキームの概要を示す図である。

[図3]図3は、本発明の実施の形態に係る放送局の構成を示す機能ブロック図である。

[図4]図4は、本発明の実施の形態に係る契約情報管理DBの契約情報管理テーブルの構成を示す図である。

[図5]図5は、本発明の実施の形態に係るワーク鍵DBのワーク鍵管理テーブルの構成を示す図である。

[図6]図6は、本発明の実施の形態に係るコンテンツ属性情報DBのコンテンツ属性情報管理テーブルの構成を示す図である。

[図7]図7は、本発明の実施の形態に係るコンテンツ鍵DBのコンテンツ鍵管理テーブルの構成を示す図である。

[図8]図8は、本発明の実施の形態に係るコンテンツDBのコンテンツ管理テーブルの構成を示す図である。

[図9]図9は、本発明の実施の形態に係るEMMの構成を示す図である。

[図10]図10は、本発明の実施の形態に係るECM-Kw、ECM-Kcの構成を示す図である。

[図11]図11は、本発明の実施の形態に係るKc伝送用ECMの構成を示す図である。

[図12]図12は、本発明の実施の形態に係る端末装置の構成を示す図である。

[図13]図13は、本発明の実施の形態に係るカード管理情報DBの共通情報テーブ

ルの構成を示す図である。

[図14]図14は、本発明の実施の形態に係るカード管理情報DBの事業者別情報テーブルの構成を示す図である。

[図15]図15は、本発明の実施の形態に係るTLの構成を示す図である。

[図16]図16は、本発明の実施の形態に係るライセンスの構成を示す図である。

[図17]図17は、本発明の実施の形態に係る放送局における契約処理、端末装置およびICカードにおけるEMM受信処理を示すフローチャートである。

[図18]図18は、本発明の実施の形態に係る放送局におけるコンテンツ送出処理を示すフローチャートである。

[図19]図19は、本発明の実施の形態に係る端末装置およびICカードにおけるコンテンツ蓄積処理を示すフローチャートである。

[図20]図20は、本発明の実施の形態に係るライセンス変換不可時にユーザに提示するメッセージを示す図である。

[図21]図21は、本発明の実施の形態に係るICカードにおけるライセンス変換可否判定処理を示すフローチャートである。

[図22]図22は、本発明の実施の形態に係る端末装置およびICカードにおけるコンテンツ利用処理を示すフローチャートである。

[図23]図23は、本発明の実施の形態の変形例に係る端末装置の構成を示す図である。

[図24]図24は、本発明の実施の形態の変形例に係るKc伝送用ECMの構成を示す図である。

[図25]図25は、本発明の実施の形態の変形例に係るTLの構成を示す図である。

[図26]図26は、本発明の実施の形態の変形例に係るPPVコンテンツの重複購入検出時にユーザに提示するメッセージを示す図である。

[図27]図27は、本発明の実施の形態の変形例に係る別端末でのライセンス取得済みによるライセンス取得不可時にユーザに提示するメッセージを示す図である。

[図28]図28は、実施の形態2に係る放送局の機能ブロック図である。

[図29]図29は、実施の形態2に係る送出装置のコンテンツ属性情報DBに記録され

ているコンテンツ属性情報管理テーブルの一例を示す図である。

[図30]図30は、実施の形態2に係る送出装置のコンテンツDBに記録されているコンテンツ管理テーブルの一例を示している。

[図31]図31は、実施の形態2に係る送出装置から送信されるKc伝送用ECMのデータ構成の一例を示す参考図である。

[図32]図32は、実施の形態2に係る受信装置のシステム構成を示す参考図である。

[図33]図33は、実施の形態2に係る受信装置側のICカードの取り込み履歴DBに記録されている取り込み履歴テーブル(IL:Import List)の一例を示す参考図である。

[図34]図34は、実施の形態2に係る放送局における送出装置が、コンテンツを送出する動作手順を示すフローチャートである。

[図35]図35は、実施の形態2に係る端末装置およびICカードにおけるコンテンツ受信および暗号変換処理を示すフローチャートである。

[図36]図36は、実施の形態2に係る端末装置における暗号変換可否判定処理(図35のS3501に対応)における動作手順を示すフローチャートである。

[図37]図37は、実施の形態2に係る端末装置およびICカードにおけるライセンス取り込み時における処理手順を示すフローチャートである。

[図38]図38は、実施の形態2に係る受信装置において、図37で示したライセンス取り込み可否判定(ステップS3702に対応)の具体的な動作手順を示すフローチャートである。

[図39]図39は、変形例に係るICカードが管理するPPC(都度購入コンテンツ)用の取り込み履歴テーブル(IL:Import List)の図である。

[図40]図40は、変形例に係る送出装置からの受信装置に配信されるKc伝送用ECMの一例を示す参考図である。

[図41]図41は、変形例に係る受信装置でのPPCのライセンス取り込みにおける処理手順を示すフローチャートである。

[図42]図42は、図41で示したライセンス取り込み可否判定(ステップS4102に対応)の具体的な動作手順を示すフローチャートである。

符号の説明

- [0024] 1 コンテンツ配信システム
- 101 放送局
 - 102 端末装置
 - 103 ICカード
 - 104 デジタル放送
 - 105 通信ネットワーク
 - 201 スクランブル鍵Ks
 - 203, 502, 1406 ワーク鍵Kw
 - 205, 703, 1606 コンテンツ鍵Kc
 - 207, 252, 406, 1302 マスタ鍵Km
 - 301 契約情報管理DB
 - 302 ワーク鍵DB
 - 303 コンテンツ属性情報DB
 - 304 コンテンツ鍵DB
 - 305 コンテンツDB
 - 306 通信部
 - 307 契約処理部
 - 308 EMM生成部
 - 309 EMM暗号化部
 - 310, 2801 ECM生成部
 - 311 ECM暗号化部
 - 312 コンテンツ符号化部
 - 313 多重化部
 - 314 コンテンツ暗号化部
 - 315 コンテンツ送出部
 - 900 EMM
 - 1000 ECM-Kw
 - 1020 ECM-Kc

1100, 2400 Kc伝送用ECM
1201 送受信部
1202 分離部
1203 蓄積部
1204 蓄積管理部
1205 コンテンツ復号部
1206 コンテンツ利用部
1207, 1213 カードI/F部
1208 ユーザI/F部
1210 カード管理情報DB
1211 変換履歴DB
1212 ライセンスDB
1214 ECM/EMM復号部
1215 ECM/EMM処理部
1216 ライセンス変換処理部
1217 ライセンス処理部
1500, 2500 TL
1600 ライセンス
3201 ECM再暗号化部
3202 ライセンス取り込み処理部
3203 取り込み履歴DB

発明を実施するための最良の形態

[0025] 以下、本発明における実施の形態について、図面を用いて詳細に説明する。

[0026] (実施の形態1)

図1は、本発明における実施の形態に関わる、デジタル権利管理システムを用いたコンテンツ配信システム1の全体の概略構成を示す図である。

[0027] このコンテンツ配信システム1は、デジタル放送を通じて放送局に設置された送出装置から送出される暗号化コンテンツを、セキュアに利用制御を行いつつ、ユーザが

端末装置において利用することが可能なシステムであって、コンテンツやコンテンツのライセンスなどを配信する放送局101と、コンテンツを利用する端末装置102と、端末装置102とともにコンテンツの利用に用いるICカード103と、これらを相互に接続するデジタル放送104、および、通信ネットワーク105とから構成されている。

- [0028] なお、端末装置102は複数あって良いが、図1では簡単のため、1つの端末装置102のみをその代表として示している。
- [0029] 放送局101は、暗号化されたコンテンツ(以下、暗号化コンテンツ)や、暗号化コンテンツを復号するための暗号鍵などを配信する送出装置などを有する。
- [0030] 端末装置102は、デジタル放送104や通信ネットワーク105などから暗号化コンテンツを受信するとともに、暗号化コンテンツを復号するためのライセンスを受信し、暗号化コンテンツを復号してコンテンツを利用するための装置である。また、端末装置102は、ICカード103を挿入するインタフェースを有しており、高いセキュリティを必要とする処理については、ICカード103と連携することにより処理を実行する。
- [0031] ICカード103は、耐タンパ化されたハードウェアモジュールである。具体的には、ICカード103は、国内デジタル放送の標準CASが実装されたB-CASカードのような高度なセキュリティを有するカードや、SD(Secure Digital)カードにセキュリティプロセッサが搭載されたようなモジュールなどがあげられる。
- [0032] デジタル放送104は、BS(Broadcasting Satellite)デジタル放送、CS(Communication Satellite)デジタル放送、地上デジタル放送などの無線によるデジタル放送や、デジタルCATVなどの有線によるデジタル放送である。
- [0033] 通信ネットワーク105は、放送局101と端末装置102とを相互に接続するネットワークである。例えば、通信ネットワーク105は、ADSL(Asymmetric Digital Subscriber Line)、FTTH(Fiber To The Home)、双方向デジタルCATV、IEEE802.11gなどの高速インターネット網である。
- [0034] なお、放送局101および端末装置102の構成については、後で図を用いて詳細に説明する。
- [0035] ここで、サーバ型放送方式における限定再生方式の暗号スキームについて、図2を用いて説明する。

- [0036] 図2において、コンテンツや暗号鍵を送出する送信側200と、コンテンツや暗号鍵を受信する受信側250に分けて説明する。
- [0037] 送信側200において、コンテンツは、スクランブル鍵Ks201と呼ばれる暗号鍵によってスクランブル、すなわち、暗号化(202)される。コンテンツのスクランブルについては、MPEG-2トランスポートストリーム(Transport Stream、以下、TSと記述)の packets 単位で、TS packets のペイロード部をスクランブルする。また、スクランブル鍵Ks201は、不正受信に対するセキュリティ向上のため、数秒おきに更新される時変鍵である。
- [0038] また、コンテンツをスクランブルするスクランブル鍵Ks201は、悪意あるユーザなどによる不正な傍受を防止するため、ワーク鍵Kw203を用いて暗号化(204)される。ワーク鍵Kw203は、従来の一般的な限定受信方式で用いられている放送事業者毎の契約単位、グループ単位に割り当てられる暗号鍵であり、ワーク鍵Kw203自体のセキュリティを確保するため、数ヶ月～数年の期間で更新されるのが一般的である。少なくともスクランブル鍵Ks201を含み、コンテンツに関連する情報を送信するためのデータ構造は、ECM(Entitlement Control Message)と呼ばれ、MPEG-2 Systems(IEC/ISO13818-1)のプライベートセクションとして構成される。ワーク鍵Kw203で暗号化されたECMは、ECM-Kwと呼ばれ、放送コンテンツのリアルタイム視聴において利用する。
- [0039] また、スクランブル鍵Ks201は、コンテンツ鍵Kc205でも暗号化(204)される。コンテンツ鍵Kc205は、コンテンツ単位に割り当てられる暗号鍵であり、ECM-Kwと同様、MPEG-2 Systemsのプライベートセクションとして構成される。少なくともスクランブル鍵Ks201を含むECMを、コンテンツ鍵Kc205で暗号化したものをECM-Kcと呼び、放送コンテンツの蓄積視聴(サーバ型放送方式におけるTypeIコンテンツ)において利用する。
- [0040] さらに、コンテンツ鍵Kc205についても、悪意あるユーザなどによる不正な傍受を防止するため、ワーク鍵Kw203で暗号化(206)される。コンテンツ鍵Kc205を含み、ワーク鍵Kw203で暗号化されたECMをKc伝送用ECMと呼び、放送コンテンツの蓄積視聴において利用する。Kc伝送用ECMは、ECM-Kw、および、ECM-

Kcと同様に、MPGE-2 Systemsのプライベートセクションとして構成されるものである。

- [0041] ECM-KwやKc伝送用ECMを暗号化するワーク鍵Kw203は、コンテンツの利用に先立って送信側200と受信側250とで共有しておく必要があるため、EMM(Entitlement Management Message)と呼ばれるデータ構造を利用して両方で共有する。このとき、スクランブル鍵Ks201やコンテンツ鍵Kc205と同様、盗聴防止のため、マスタ鍵Km207と呼ばれる端末装置102固有の暗号鍵で暗号化(208)する。このマスタ鍵Km207についても、送信側200と受信側250で予め共有しておく必要があるが、受信側250のマスタ鍵Km252は、端末装置102のセキュアな部分や、セキュリティモジュールと呼ばれるハードウェア的に耐タンパ化されたモジュールなどに出荷時などに予め書き込まれることで設定される。
- [0042] なお、ECM-Kw、ECM-Kc、Kc伝送用ECM、EMMのデータ構造の例については、後で図を用いて詳細に説明する。
- [0043] また、本暗号スキームにおいて、端末装置102では、マスタ鍵Km207、ワーク鍵Km203など、特にセキュリティを必要とする情報の管理および処理を、ICカードで行うようにするようにしても良い。
- [0044] また、本暗号スキームで使用する暗号アルゴリズムとしては、AES(Advanced Encryption Standard)などの共通鍵暗号方式が用いられる。
- [0045] また、ワーク鍵Kw203については、送信側200と受信側250との間でSAC(Secure Authenticated Channel)を確立し、通信ネットワーク105を介してワーク鍵Kw203を共有するようにしても良い。
- [0046] 以上のように生成された暗号化コンテンツ、ECM-Kw、ECM-Kc、Kc伝送用ECM、および、EMMは、MPEG-2 TSパケット化され、必要に応じてPSI(Program Specific Information)/SI(Service Information)などのデータと多重化(209)された後、受信側250に送信される。
- [0047] 一方、受信側250では、送信側200から送出されたMPEG-2 TSパケットを受信し、これらを分離(251)して、暗号化コンテンツ、ECM-Kw、ECM-Kc、Kc伝送用ECM、および、EMMを取得する。

- [0048] この暗号化されたEMMは、受信側250で予め保持しているマスタ鍵Km252を用いて復号(253)し、ワーク鍵Kw203を取得する。このワーク鍵Kw203は、受信側250の不揮発性メモリなどで保持される。
- [0049] コンテンツをリアルタイム視聴する場合、ECM-Kwを取得して、ワーク鍵Kw203により暗号化されたECM-Kwを復号(255)して、スクランブル鍵Ks201を取得する。スクランブル鍵Ks201によって暗号化コンテンツを復号(256)して、コンテンツを利用することが可能となる。
- [0050] 一方、コンテンツを蓄積視聴する場合、図示しない蓄積部に記録された暗号化コンテンツ、ECM-Kc、Kc伝送用ECMを読み出す。Kc伝送用ECMについては、送信側200からは繰り返し送出されるが、受信側250では1回だけ取得すれば良い。なお、ECM-Kwは、リアルタイム視聴時のみで使用されるため、受信側250では蓄積されない。
- [0051] リアルタイム視聴の場合において説明した方法で取得したワーク鍵Kw203を用いて、暗号化されたKc伝送用ECMを復号(254)して、コンテンツ鍵Kc205を取得する。これによりコンテンツ鍵Kc205によりECM-Kcを復号(255)し、暗号化コンテンツを復号(256)して、コンテンツを利用することが可能となる。
- [0052] 以上、図2を用いて、サーバ型放送方式の限定再生方式の暗号スキームについて説明した。以降、本発明における実施の形態では、図2で説明した暗号スキームに基づくデジタル権利管理システムについての説明を行う。
- [0053] このようなコンテンツ配信システム1において、デジタル放送104を通じて、コンテンツ(番組)、ライセンスが配信され、端末装置102において、コンテンツ、ライセンスをHDDなどに蓄積し、ライセンスに基づきコンテンツを利用する処理を、図3～図22の図面を用いて詳細に説明する。
- [0054] 図3は、図1に示す放送局101の構成を示す機能ブロック図である。
- 放送局101は、契約情報を管理する契約情報管理DB301と、ワーク鍵を管理するワーク鍵DB302と、コンテンツに関連する属性情報を管理するコンテンツ属性情報DB303と、コンテンツ毎に割り当てられるコンテンツ鍵を管理するコンテンツ鍵DB304と、映像、音声などのコンテンツを管理するコンテンツDB305と、端末装置102と

のインタフェースを提供する通信部306と、ユーザの契約情報を管理する契約処理部307と、端末装置102毎の個別情報を生成するEMM生成部308と、EMMを暗号化するEMM暗号化部309と、全端末装置102に共通な情報を生成するECM生成部310と、ECMを暗号化するECM暗号化部311と、コンテンツをエンコードするコンテンツ符号化部312と、MPEG-2 TSを多重化する多重化部313と、映像、音声などのTSパケットを暗号化するコンテンツ暗号化部314と、TS化されたコンテンツを送出するコンテンツ送出部315とで構成されている。

- [0055] 契約情報管理DB301は、ユーザのコンテンツの視聴契約に関する情報を管理するためのデータベースである。具体的には、契約情報管理DB301は、図4に示すように、ICカード103毎の視聴契約に関連する情報や、マスタ鍵Km207を一元管理する契約情報管理テーブル400を有する。契約情報管理DB301は、主として、EMM生成部308が、端末装置102毎に視聴契約情報を配信するためのEMMを生成する際に参照する。
- [0056] カードID401は、端末装置102に挿入するICカード103を一意に識別し、契約処理を行ったICカード103に対してEMM900を送出するための宛て先となる情報である。
- [0057] ティア契約ID402は、放送局101が提供するサービスに対する月極め契約(サブスクリプション)の識別をするためのIDであり、一種の契約形態を示している。例えば、スポーツに関するコンテンツを視聴できる「スポーツコンテンツパック」、映画コンテンツを視聴できる「映画コンテンツパック」などがあげられる。
- [0058] PPV契約ID403は、放送局101が提供するサービスに対するペイ・パー・ビューの視聴契約を識別するためのIDであり、ティア契約ID908と同様、一種の契約形態を示している。
- [0059] 有効期限404は、放送局101との契約期間を示すものであり、有効期限904までは、当該放送局101のコンテンツを利用することが可能となる。
- [0060] 蓄積暗号鍵Km' 405は、端末装置102において、コンテンツやライセンス(ECMなど)をHDDなどに蓄積する場合に、コンテンツやライセンスを取得した端末装置102、すなわち、ICカード103に、コンテンツやライセンスをバインドする際に用いる。

- [0061] マスタ鍵Km406は、ICカード103固有の暗号鍵であり、EMMを暗号化する場合に用いる。ICカード103では出荷時に埋め込まれる。
- [0062] 例えば、図4では、カードID401が「CARD-ID-1」なるICカード103は、ティア契約ID402が「TIERCONT-ID-1」、PPV契約ID403が「PPVCONT-ID-1」であるサービスに加入しており、有効期限404が「2004/4/1～2005/3/31」であり、蓄積暗号鍵Km'405が「0x111...111」、マスタ鍵Km406が「0x111...11」であることを示している。
- [0063] ワーク鍵DB302は、ユーザが事業者と視聴契約を行った場合に送出するECMを暗号化する鍵を管理するためのデータベースであって、ワーク鍵管理テーブル500を有する。ワーク鍵DB302は、ECM-Kw、Kc伝送用ECMを暗号化する際に、ワーク鍵Kw203を提供したりする場合に用いられる。
- [0064] 具体的には、ワーク鍵DB302は、図5に示すように、ワーク鍵ID501、ワーク鍵Kw502、ワーク鍵利用開始日503の組を管理するワーク鍵管理テーブル500を管理する。
- [0065] 例えば、図5では、ワーク鍵ID501「WK-ID-1」に対応するワーク鍵Kw502が「0x123...cdf」であり、ワーク鍵Kw502の利用開始日を示すワーク鍵利用開始日503が「2003/11/24」であることを示している。また、ワーク鍵ID501は、暗号化されたECMにおいて、暗号化に用いたワーク鍵Kw203を特定するために用いられる情報であり、ECM-Kwのワーク鍵ID1104や、Kc伝送用ECMのワーク鍵ID1004に設定される。
- [0066] コンテンツ属性情報DB303は、コンテンツの利用条件や、当該コンテンツを視聴可能な契約の種類など、コンテンツ利用に関する種々の情報を管理するためのデータベースである。具体的には、コンテンツ属性情報DB303は、図6に示すように、コンテンツ配信システム1内でコンテンツを一意に特定するためのコンテンツID601と、コンテンツ配信システム1内でライセンスを一意に特定するためのライセンスID602と、利用条件603と、契約情報604と、ライセンス変換期限605とを有するコンテンツ属性情報管理テーブル600を備えている。尚、請求の範囲におけるライセンス取り込み期限は、本実施の形態の説明におけるライセンス変換期限と対応しているものである。

- 。
- [0067] 例えば、コンテンツID601が「CONTENT-ID-1」、ライセンスID602が「LICENSE-ID-1」であるコンテンツは、利用条件603が「有効期限1ヶ月」、契約情報604が「TIERCONT-ID-1」、ライセンス変換期限605が「2004/4/30」であることから、放送局101と「TIERCONT-ID-1」なるサービスを契約し、「2004/4/30」までにライセンスを取得する処理を行った場合、コンテンツを蓄積してから1ヶ月間は当該コンテンツが再生可能であることを示している。なお、ライセンス変換期限605に関わるライセンス変換処理については、端末装置102の構成について説明する際に、詳細に説明する。
- [0068] また、コンテンツID601が「CONTENT-ID-2」なるコンテンツについては、契約情報604が「TIERCONT-ID-1、TIERCONT-ID-2」であることから、このコンテンツを視聴するためには、放送局101と「TIERCONTENT-ID-1」または「TIERCONT-ID-2」の少なくともどちらかのサービスを契約していることが必要となる。また、コンテンツID601が「CONTENT-ID-4」なるコンテンツについては、契約情報604が「PPVCONT-ID-1」であることから、このコンテンツがPPVコンテンツであることが示されている。
- [0069] コンテンツ鍵DB304は、端末装置102に蓄積されたコンテンツを利用するためのライセンス毎(すなわち、コンテンツ毎)に割り当てられる暗号鍵を管理するデータベースである。
- [0070] 具体的には、コンテンツ鍵DB304は、コンテンツ配信システム1においてコンテンツをユニークに識別するための識別子であるコンテンツID701、コンテンツ配信システム1においてライセンスをユニークに識別するための識別子であるライセンスID702、ライセンスID702に設定するコンテンツ鍵Kc703から構成されるコンテンツ鍵管理テーブル700を有する。
- [0071] 例えば、図7では、コンテンツ701が「CONTENT-ID-1」に対応するライセンスID702が、「LICENSE-ID-1」であり、これらに対応するコンテンツ鍵Kc703が、「0x123...cdf」であることを示している。
- [0072] コンテンツDB305は、コンテンツを蓄積するためのデータベースである。具体的に

は、コンテンツDB305は、図8に示すように、コンテンツ配信システム1内でコンテンツを一意に特定するためのコンテンツID801と、コンテンツの名前を示すコンテンツ名称802と、コンテンツをデジタル放送で配信する日時を示す放送日時803と、コンテンツ毎のコンテンツDB305におけるファイルの位置を示すファイル名804とを有するコンテンツ管理テーブル800を備えている。

[0073] 例えば、コンテンツID801が「CONTENT-ID-1」のコンテンツは、コンテンツ名称802が「マンデースポーツ」であり、放送日時803が「2004/4/8

21:00:00」、コンテンツDB305におけるファイル名804はURI(Uniform Resource Identifier)が「/SPORT/.../MONSPORTS.VC」(「...」はURIの一部が省略されていることを示している)であることを示している。

[0074] なお、コンテンツ管理テーブル800は、アナログVCR(Video Cassette Recorder)であってもよいし、コンテンツ管理テーブル800に代わり、ライブ放送(生放送)などを撮影するビデオカメラなどであっても良い。

[0075] 通信部306は、通信ネットワーク105を通じて、端末装置102と通信するための部である。

[0076] 契約処理部307は、端末装置102からの視聴契約の申し込みを処理する部である。

具体的には、契約処理部307は、Webブラウザなどを通じて放送局101との視聴契約を受け付け、ユーザ(端末装置102)に対する視聴契約情報を、契約情報管理DB301に登録する。

[0077] EMM生成部308は、ワーク鍵Kw203やユーザの契約情報などを含むEMMを生成する部である。

[0078] 具体的には、EMM生成部308は、主として新規契約や契約変更が行われたユーザ(端末装置102、すなわち、ICカード103)に対して、契約情報管理DB301から当該ユーザの契約内容であるティア契約ID402、PPV契約ID403、有効期限404などを読み出し、EMMに設定する。

[0079] ここで、図9を用いて、EMMのデータ構造についての詳細な説明を行う。

図9は、主としてワーク鍵Kw201やユーザ毎(ICカード103毎)の情報を伝送する

EMMのデータ構造の一例を示す図である。

- [0080] 図9に示したEMM900は、カードID902、事業者ID903、有効期限904、ワーク鍵ID905、ワーク鍵Kw906、蓄積暗号鍵Km'907、ティア契約ID908、PPV契約ID909、改ざん検出910とから構成されている。また、MPEG-2 Systemsのプライベートセクション形式でトランスポートストリームに多重化するため、セクションヘッダ901、セクションテラ(誤り検出)911が付加されている。EMM900に示したデータの大部分は、ICカード103に蓄積され、管理される。
- [0081] カードID902は、コンテンツ配信システム1において、端末装置102に挿入するICカード103を一意に識別し、契約処理を行ったICカード103に対してEMM900を送出するための宛て先となる情報である。
- [0082] 事業者ID903は、コンテンツ配信システム1において、サービスを提供する事業者を識別するコードであって、後述するワーク鍵ID905とともに参照される。
- [0083] 有効期限904は、放送局101との契約期間を示すものであり、有効期限904までは、当該放送局101のコンテンツを利用することが可能となる。
- [0084] ワーク鍵ID905は、ECMを暗号化するワーク鍵Kw203を識別するための情報であり、ICカード103で暗号化されたECMを復号する際には、ワーク鍵ID905と同様の情報がECMの非暗号化部分に設定されるので、ワーク鍵ID905を参照することにより、どのワーク鍵Kw203を用いて暗号化されたECMを復号すれば良いかを判別することができる。
- [0085] ワーク鍵Kw906は、放送局101との契約に対してユーザに与えられる暗号化であり、ICカード103で暗号化されたECM-Kw、および、Kc伝送用ECMを復号する際に用いる。
- [0086] 蓄積暗号鍵Km'907は、端末装置102において、コンテンツやライセンス(ECMなど)をHDDなどに蓄積する場合に、コンテンツやライセンスを取得した端末装置102、すなわち、ICカード103に、コンテンツやライセンスをバインドする際に用いる。
- [0087] ティア契約ID908は、放送局101が提供するサービスに対する月極め契約(サブスクリプション)の識別をするためのIDであり、「標準パック」、「プレミアムパック」などの放送局101との契約形態を示している。

- [0088] PPV契約ID909は、放送局101が提供するサービスに対するペイ・パー・ビューの視聴契約を識別するためのIDであり、ティア契約ID908と同様、一種の契約形態を示している。
- [0089] 改ざん検出910は、暗号化したEMM900の改ざんを検出するためのハッシュ値が設定される。ハッシュアルゴリズムは、AESのCBCモードで暗号化した結果であるMAC(Message Authentication Code)や、SHA-256などを用いる。
- [0090] なお、ここでは、ティア契約、PPV契約については、ティア契約ID908、PPV契約ID909をそのままEMM900に設定する場合の例を説明したが、それぞれのIDをビットマップなどで表現したものをEMM900で配信し、伝送すべき情報量とICカード103での保持すべき情報量を削減するようにしても良い。
- [0091] また、ここでは、ワーク鍵Kw203は事業者毎に割り当てる場合の例を説明したが、ティア契約ID毎などの契約毎にワーク鍵Kw203を割り当てるようにしても良い。
- [0092] 以上、図9を用いて、EMM900のデータ構造についての詳細な説明を行った。
- EMM暗号化部309は、AESなどを用いて、EMM生成部308で生成したEMM900を暗号化する部である。
- [0093] 具体的には、EMM暗号化部309は、EMM生成部308で生成したEMM900を、契約情報管理DB301から取得したマスタ鍵Km207で暗号化し、多重化部313に送信する。EMM900を暗号化するにあたっては、暗号化モードは、CBC(Cipher Block Chaining)+OFB(Output FeedBack)を用いる。
- [0094] ECM生成部310は、スクランブル鍵Ks201などを含むECMを生成する部である。具体的には、ECM生成部310は、上流システムからの指示により、コンテンツの送出に合わせてECM-Kw、ECM-Kc、Kc伝送用ECMを生成する。ECM-Kw、および、ECM-Kcの生成については、コンテンツのセキュリティを堅固なものとするため、数秒おきにスクランブル鍵Ksを生成して、ECM-Kw、ECM-Kcに設定する。Kc伝送用ECMの生成については、コンテンツ属性情報DB303、および、コンテンツ鍵DB304から、利用条件603やコンテンツ鍵Kc703などを取得して、Kc伝送用ECMに設定する。また、生成したスクランブル鍵Ks201を、コンテンツを暗号化するコンテンツ暗号化部314に送信する。

- [0095] ここで、図10～図11を用いて、ECM-Kw、ECM-Kc、Kc伝送用ECMのデータ構造についての詳細な説明を行う。
- [0096] 図10は、主としてスクランブル鍵Ks201を伝送するECM-KwおよびECM-Kcのデータ構造の一例を示す図である。
- [0097] 図10に示したECM-Kw1000、および、ECM-Kc1020は、スクランブル鍵Ks201やコンテンツに関する情報の伝送に用いられる情報であり、事業者ID1002、ワーク鍵ID1003、コンテンツID1004、スクランブル鍵Ks1005、契約判定情報1006、改ざん検出1007とから構成されている。また、MPEG-2 Systemsのプライベートセクション形式でトランスポートストリームに多重化するため、セクションヘッダ1001、セクションテラ(誤り検出)1007が付加されている。
- [0098] 事業者ID1002は、コンテンツ配信システム1において、サービスを提供する事業者を識別するコードであって、次に述べるワーク鍵ID1003とともに参照される。
- [0099] ワーク鍵ID1003は、ECMを暗号化するワーク鍵Kw203を識別するための情報であり、ECMの非暗号化部分に設定される。ICカード103で、暗号化されたECMを復号する場合には、ワーク鍵ID1003を参照することにより、どのワーク鍵Kw203を用いてECMを復号すれば良いかを判別することができる。
- [0100] コンテンツID1004は、コンテンツ配信システム1内でコンテンツに対して一意に割り当てられる識別子であり、コンテンツの識別のために用いる。
- [0101] スクランブル鍵Ks1005は、コンテンツのTSパケットのペイロード部を暗号化する暗号鍵である。端末装置102が、数秒おきに変更されるスクランブル鍵Ks1005を取得するために要する時間を短縮するため、一般的にはスクランブル鍵Ks1005に複数の暗号鍵を設定する。
- [0102] 契約判定情報1006は、当該コンテンツの属性を示す情報であり、端末装置102でコンテンツを視聴する場合に、当該コンテンツを視聴するための契約がなされているか否かを判定するために用いる。
- [0103] 改ざん検出1007は、暗号化されるECMの改ざんを検出するためのハッシュ値が設定される。ハッシュアルゴリズムは、EMM900の場合と同様、AESのCBC-MACや、SHA-256などを用いる。

- [0104] 次に、図11は、主として蓄積視聴のためのECM-Kc1020を復号するためのコンテンツ鍵Kc205を伝送するKc伝送用ECMのデータ構造の一例を示す図である。
- [0105] 図11に示したKc伝送用ECM1100は、コンテンツ鍵Kc205やコンテンツの利用条件(ライセンス)の伝送に用いられる情報であり、事業者ID1102、サービスタイプ1103、ワーク鍵ID1104、契約判定情報1105、ライセンス変換期限1106、ライセンスID1107、ライセンス有効期限1108、コンテンツ鍵Kc1109、利用可能回数1110、書き出し可能回数1111、改ざん検出1112とから構成されている。また、ECM-Kw1000およびECM-Kc1020と同様に、セクションヘッダ1101、セクションテラ(誤り検出)1113が付加されている。
- [0106] 事業者ID1102、ワーク鍵ID1104、契約判定情報1105、改ざん検出1112については、ECM-Kc1000、および、ECM-Kc1020における事業者ID1002、ワーク鍵ID1003、契約判定情報1006、改ざん検出1008の説明と同様であるので、ここでは説明を省略する。
- [0107] サービスタイプ1103は、Kc伝送用ECM1100を含むコンテンツが、ティア契約で視聴可能なコンテンツであるのか、PPV契約であって、別途購入処理を行うことによって視聴可能なコンテンツであるのか、を識別するためのフラグである。本発明の実施の形態においては、ティア契約を「TIERCONT」、PPV契約を「PPVCONT」として、以下の説明を行う。
- [0108] ライセンス変換期限1106は、ICカード103において、Kc伝送用ECM1100を変換して、蓄積視聴用のライセンスを取得する処理の期限を示すものである。ライセンス変換とは、Kc伝送用ECM1100に含まれる情報を用いて、蓄積視聴用のライセンスをフォーマット変換により生成する処理を指す。このライセンス変換期限1106を経過した場合には、Kc伝送用ECM1100から蓄積視聴に必要なライセンスを取得することはできず、ライセンス変換期限1106経過後に、別途、通信などを用いて取得する必要がある。
- [0109] ライセンスID1107は、変換したライセンスをコンテンツ配信システム1内で一意に識別するためのコードであり、ICカード103において、ライセンスの変換履歴としても用いる。

- [0110] ライセンス有効期限1108は、当該ライセンスにより、コンテンツを視聴可能な期限を示すものである。
- [0111] コンテンツ鍵Kc1109は、コンテンツ単位で割り当てられる16バイト長の暗号鍵であり、ライセンスに含まれる暗号鍵である。
- [0112] 利用可能回数1110は、当該ライセンスにより、コンテンツを視聴可能な回数を示すものである。
- [0113] 書き出し可能回数1111は、当該ライセンスにより、コンテンツを蓄積媒体に書き出すことが可能な回数を示すものである。
- [0114] なお、ワーク鍵Kw203で暗号化されたリアルタイム視聴用のECM-Kc1000と、コンテンツ鍵Ks205で暗号化された蓄積視聴用のECM-Kc1020のフォーマットは同一であり、暗号化を行う暗号鍵(ワーク鍵Kw203とコンテンツ鍵Ks205)と、セクションヘッダ1001に記載されるセクション識別情報(テーブルID、テーブルIDエクステンションなど)やTSパケットのPID(Packet ID)などが異なる。
- [0115] また、ライセンス変換期限1106を、ライセンス有効期限1108とは別に設けることによって、端末装置102にコンテンツおよびライセンスを大量に蓄積し、短期の視聴契約を行うことによって、視聴契約期間以外に蓄積した過去のライセンスも含めて、短期間に大量のライセンスを取得されてしまうという課題を解決することができる。この場合には、ライセンス変換期限1106は、比較的短い期限を設定すると良い。また、この目的のためには、必ずしもライセンス(Kc伝送用ECM)毎にライセンス変換期限1106を設ける必要はなく、システム固定値としてICカード103などがあらかじめ保持しておくようにしても良い。
- [0116] 以上、図10～図11を用いて、ECM-Kw1000、ECM-Kc1020、Kc伝送用ECM1100のデータ構造についての詳細な説明を行った。
- [0117] ECM暗号化部311は、AESなどを用いて、ECM生成部310で生成したECMを暗号化する部である。具体的には、ECM暗号化部311は、ECM生成部310で生成したECM-Kw1000、および、Kc伝送用ECM1100を、ワーク鍵DB302から取得したワーク鍵Kw203で暗号化する。合わせて、ECM生成部310で生成したECM-Kc1020を、コンテンツ鍵DB304から取得したコンテンツ鍵Kc205で暗号化する

。各ECMを暗号化するにあたっては、暗号化モードは、CBC+OFBを用いる。ECM暗号化部311は、このように暗号化した各ECMを、多重化部313に送信する。

[0118] コンテンツ符号化部312は、端末装置102に送出するコンテンツをコンテンツDB305から読み出し、コンテンツをMPEG形式で符号化する部である。

[0119] 具体的には、コンテンツ符号化部312は、MPEGストリームを生成するリアルタイムエンコーダであって、上流システム(例えば、番組運行管理システムなど)の指示により、コンテンツDB305から映像、音声などを読み出し、映像、音声、データなどのMPEG-2やMPEG-4のES(Elementary Stream)を生成する。さらに、これらのESを含むPES(Packetized Elementary Stream)パケットを生成し、最後にMPEG-2 TSパケット化して、多重化部313に送出する。

[0120] 多重化部313は、コンテンツ符号化部312から受け取った映像、音声、データなどを含むトランスポートストリームと、ECM暗号化部311から受け取ったECMのトランスポートストリームと、EMM暗号化部309から受け取ったEMM900のトランスポートストリームとを多重化し、多重化されたトランスポートストリームをコンテンツ暗号化部314に送出する部である。具体的には、多重化部313は、コンテンツ符号化部312から受信したTSパケット化されたコンテンツと、ECM暗号化部311から受信したTSパケット化されたECM-Kw1000、ECM-Kc1020、Kc伝送用ECM1100と、EMM暗号化部309から受信したTSパケット化されたEMM900とをTS多重化して、端末装置102に送信するための多重化トランスポートストリームを生成する。

[0121] コンテンツ暗号化部314は、AESなどを用いてコンテンツを暗号化することにより、コンテンツのスクランブルを行う部である。具体的には、コンテンツ暗号化部314は、TSパケットのアダプテーションフィールドを除くペイロード部を、ECM生成部310から取得したスクランブル鍵Ks201を用いて、CBC+OFBモードによって暗号化(スクランブル)する。

[0122] コンテンツ送出部315は、コンテンツ暗号化部314において暗号化されたTSパケットを、端末装置102に送出する部である。具体的には、コンテンツ送出部315は、コンテンツ暗号化部314から受け取ったトランスポートストリームを、放送波としてネットワーク103を通じて端末装置102に送出する。

- [0123] なお、ここでは、コンテンツDB305に蓄積されたコンテンツを読み出し、コンテンツ符号化部312においてリアルタイムエンコードする場合の例を示したが、あらかじめオフラインでPES(ES)あるいはTSを生成しておき、コンテンツDB305に蓄積しておくことにより、コンテンツ送出時にコンテンツ符号化部312におけるエンコード処理を省略するようにしても良い。
- [0124] 以上、図3～図11を用いて、放送局101の構成についての詳細な説明を行った。一方、図12は、図1に示す端末装置102、および、ICカード103の構成を示す機能ブロック図である。
- [0125] まず、端末装置102を構成する機能ブロックについての説明を行う。
- 送受信部1201は、デジタル放送104、および、通信ネットワーク105を通じて、放送局101からのコンテンツやライセンスを受信したり、放送局101と通信したりするための処理部である。
- [0126] 分離部1202は、MPEG-2 TSにより多重化された暗号化コンテンツを取得し、コンテンツとECMなどとを分離するための処理部である。
- [0127] 具体的には、分離部1202は、送受信部1201が受信したトランスポートストリームに含まれるPAT(Program Association Table)、PMT(Program Map Table)などのPSI情報を参照して、コンテンツの映像、音声、データや、ECM-Kw1000、ECM-Kc1020、Kc伝送用ECM1100を含むTSパケットのPIDを取得し、コンテンツとECM-Kc1020などとを分離する。コンテンツ蓄積部1203にコンテンツを蓄積する場合には、PAT、PMTなどのPSI情報から必要な情報を選択してSIT(Selection Information Table)、DIT(Discontinuity Information Table)などのPSI情報の生成を行い、受信したトランスポートストリームを、パーシャルトランスポートストリーム(以下、パーシャルTSと記述する)と呼ばれるストリームを生成する処理を行う。
- [0128] 蓄積部1203は、コンテンツやライセンスなどを蓄積するための部である。具体的には、蓄積部1203は、HDDなどの大容量不揮発性記憶媒体であり、分離部1202において受信したトランスポートストリームから生成した、映像、音声などのコンテンツやECM-Kc1020などのライセンスを含むパーシャルTSを蓄積する。

- [0129] 蓄積管理部1204は、端末装置102の蓄積部1203に蓄積するコンテンツやライセンスを管理しており、蓄積したコンテンツやライセンスの一覧などをユーザに提示するための情報を有する。
- [0130] コンテンツ復号部1205は、暗号化コンテンツを復号する部である。具体的には、コンテンツ復号部1205は、暗号化されたMPEG-2 TSのコンテンツを取得し、トランスポートストリームに含まれるPAT、PMTなどのPSI情報を参照して、コンテンツの映像、音声、データを含むTSパケットを取得する。そして、ICカード103から取得するスクランブル鍵Ks201でAES暗号化されたTSパケットのペイロード部分を復号する。
- [0131] コンテンツ利用部1206は、ICカード103から取得するスクランブル鍵Ks201とコンテンツの利用条件とを用いて、セキュアにコンテンツの利用を行うための部である。
- [0132] 具体的には、コンテンツ利用部1206は、リアルタイム視聴時においては、分離部1202から受け取ったトランスポートストリームからECM-Kw1000のTSパケットを取得し、ECM-Kw1000を再構成する。このようにして得られたECM-Kw1000をワーク鍵Kw203で復号して、コンテンツをデスクランブルするためのスクランブル鍵Ks201を取得し、コンテンツを復号する。一方、蓄積視聴時においては、蓄積部1203から読み出したトランスポートストリームから、Kc伝送用ECM1100をワーク鍵Kw203で復号して、ライセンスを取得する。そして、ライセンスに含まれる利用条件判定を行った上で、コンテンツを利用可能である場合のみ、ライセンスに含まれるコンテンツ鍵Kc205を用いて、ECM-Kc1020を復号して、スクランブル鍵Ks201を取得する。さらに、コンテンツ利用部1206は、図12に図示しないセキュアな計時部を用いて、コンテンツの利用時間などを計時することにより、利用条件に従ったコンテンツの利用を制御する。このような制御のもと、コンテンツ利用部1206は、MPGE-2あるいはMPEG-4の映像、音声、データなどのESをデコードして、図12に示さないモニタなどに出力する。
- [0133] なお、コンテンツの利用を終了した場合に、ICカード103に対して、利用終了通知を通知するようにしても良い。
- [0134] 端末装置102における第1のカードI/F部1207は、端末装置102とICカード103

とのインタフェースを提供するための部である。

- [0135] 具体的には、第1のカードI/F部1207は、ISO7816-4で規定されているT=0プロトコルやT=1プロトコルを処理し、端末装置102やICカード103の他の機能ブロックとの間で相互にデータをやりとりするための手段を提供するものである。端末装置102とICカード103との通信は、悪意あるユーザなどによる通信の傍受を防止するため、少なくともセキュリティを要する情報の授受については、端末装置102とICカード103との間で相互認証が行われ、SAC(Secure Authenticated Channel)を確立した上で行われる。
- [0136] ユーザI/F部1208は、端末装置102とユーザとのインタフェースを提供するための部である。
- [0137] 具体的には、ユーザI/F部1208は、BML(Broadcasting Markup Language)ブラウザ、Webブラウザ、レジデントアプリケーションなどのGUI(Graphical User Interface)であり、図12に示さないモニタなどを通じて、ユーザ要求を受け付けたり、ユーザにメッセージを提示したりする。
- [0138] 以上、端末装置102を構成する機能ブロックについての説明を行った。
次に、ICカード103を構成する機能ブロックについての説明を行う。
- [0139] カード情報管理DB1210は、ユーザのコンテンツの視聴契約に関する情報を管理するためのデータベースである。具体的には、カード情報管理DB1210は、全事業者で共通の視聴契約に関連する情報を管理する共通情報テーブル1300と、事業者毎の視聴契約に関する情報を管理する事業者別情報テーブル1400とを有する。
- [0140] カード情報管理DB1210の共通情報テーブル1300は、図13に示すように、カードID1301と、マスタ鍵Km1302と、蓄積暗号鍵Km'1303とを管理する。
- [0141] カードID1301は、コンテンツ配信システム1内でICカード103を一意に識別するためのIDであり、ICカード103に予め書き込まれて出荷される。
- [0142] マスタ鍵Km1302は、EMM900を暗号化する場合に用いられるカードID1301固有の暗号鍵であり、カードID1301と同様、ICカード103に予め書き込まれて出荷される。
- [0143] 蓄積暗号鍵Km'1303は、端末装置102の蓄積部1203でライセンスを蓄積する

場合に、ライセンスの取得を行ったICカード103にライセンスをバインドするための暗号鍵であり、EMM900の事業者ID903で指定されるIDである。

- [0144] 一方、カード情報管理DB1210の事業者別情報テーブル1400は、図14に示すように、事業者ID1401と、ティア契約ID1402と、PPV契約ID1403と、有効期限1404と、ワーク鍵ID1405と、ワーク鍵Kw1406とを管理する。
- [0145] 事業者ID1401は、コンテンツ配信システム1内で一意に放送局101を識別するためのIDであり、EMM900の事業者ID903で指定されるIDである。
- [0146] ティア契約ID1402は、ユーザが放送局101と月極めコンテンツの視聴契約を行ったサービスのIDであり、EMM900のティア契約ID908で指定されるIDである。
- [0147] PPV契約ID1403は、ユーザが放送局101とPPVコンテンツの契約を行ったサービスのIDであり、EMM900のPPV契約ID909で指定されるIDである。
- [0148] 有効期限1404は、放送局101との視聴契約における視聴期限を示すものであり、EMM900の有効期限904で指定される期限である。
- [0149] ワーク鍵ID1405は、コンテンツ配信システム1内で、放送局101から配布されるワーク鍵Kw203を一意に識別するためのIDであり、EMM900のワーク鍵ID905で指定されるIDである。但し、ワーク鍵Kw203の識別については、事業者ID1401とワーク鍵ID1405との組により、コンテンツ配信システム1内でユニークとなることに注意されたい。
- [0150] ワーク鍵Kw1406は、放送局101から配布されるワーク鍵Kw203であり、EMM900のワーク鍵Kw906で指定される16バイトのバイト列である。
- [0151] 例えば、図14では、事業者ID1401が「SERVICE-ID-1」である事業者との契約内容は、ティア契約ID1402が「TIERCONT-ID-1」、PPV契約ID1403が「PPVCONT-ID-1」、有効期限1404が「2004/4/1~2005/3/31」、ワーク鍵ID1405が「KW-ID-1」、ワーク鍵Kw1406が「0x111...111」であることを示しており、「SERVICE-ID-1」であるコンテンツは、ティアコンテンツ(Kc伝送用ECM1100のサービスタイプ1104が「TIERCONT」であるコンテンツ)とPPVコンテンツ(Kc伝送用ECM1100のサービスタイプ1104が「PPVCONT」であるコンテンツ)の両方のコンテンツが視聴可能である。また、事業者ID1401が「SERVICE-I

D-10」である事業者については、ティア契約ID1402が「- (未契約)」、PPV契約ID1403が「PPVCONT-ID-1」であることから、「SERVICE-ID-1」であるコンテンツは、ティアコンテンツについては視聴不可であるが、PPVコンテンツに関しては、別途購入処理を行うことによって視聴が可能である。

- [0152] なお、ここでは、ワーク鍵ID1405とワーク鍵1406の組は、最新の一組を保持する場合の例を示したが、ワーク鍵の運用を切り替える際のスムーズな移行を行うため、事業者別情報テーブル1400においては、少なくとも二組のワーク鍵を保持できるようにしておくのが望ましい。
- [0153] 変換履歴DB1211は、ライセンスの変換履歴を蓄積するためのデータベースである。具体的には、変換履歴DB1211は、Kc伝送用ECM1100に含まれる情報から、蓄積視聴用のライセンスが無制限に変換されることを防止するため、ライセンスの変換(以下、ライセンス変換と記述)が行われたことを示す変換履歴(Transformation Log、以下、TLと記述)を保持する。
- [0154] ここで、変換履歴DB1211に蓄積するTLのデータ構造の一例を、図15を用いて説明する。
- [0155] TL1500は、ライセンス変換を行ったライセンスを識別するためのライセンスID1501と、ライセンス変換が可能な期間を示すライセンス変換期限1502との組から構成されており、これらの複数組をリストとして管理している。TL1500の各レコードは、少なくとも、ライセンス変換期限1502を経過するまでは保持されるため、一度変換を行ったライセンスについては、さらなるライセンス変換を抑制することができ、その結果、1つのKc伝送用ECM1100からは、1つのライセンスのみを取得することができるので、事業者の権利を確実に保護することができる。
- [0156] ライセンスDB1212は、放送局101から取得したライセンスをセキュアに管理するためのデータベースである。具体的には、ライセンスDB1212は、放送局101から取得したライセンスを蓄積、管理するとともに、端末装置102の蓄積部1203などのICカード103の外部にライセンスを蓄積する場合において、ライセンスの改ざんなどの不正な行為を防止するため、ライセンスDB1212中のライセンスのハッシュ値を管理する。

- [0157] 第2のカードI/F部1213は、端末装置102における第1のカードI/F部1207と同様の機能ブロックであるため、ここでは説明を省略する。
- [0158] ECM/EMM復号部1214は、端末装置102から受信した、暗号化されたECM、および、暗号化されたEMM900を復号するための部である。具体的には、ECM/EMM復号部1214は、第2のカードI/F部1213から暗号化ECM-Kw1000、暗号化ECM-Kc1020、暗号化EMM900を受け取り、カード管理情報DB1210から、それぞれに対応するワーク鍵Kw203(1406)、マスタ鍵Km207(1302)を読み出し、また、ライセンスDB1212に保持されているライセンスからコンテンツ鍵Kc205を受け取り、暗号化ECM-Kw1000、暗号化ECM-Kc1020、Kc伝送用ECM1100、暗号化EMM900の暗号を復号する。
- [0159] ECM/EMM処理部1215は、平文のECMやEMMから必要な情報を抽出したり、処理したりするための部である。具体的には、ECM/EMM処理部1215は、ECM/EMM復号部1214から受け取ったECM-Kw1000、ECM-Kc1020、Kc伝送用ECM1100、EMM900を解釈し、カード管理情報DB1210の構築に必要な情報を抽出して記録したり、端末装置102がコンテンツの再生に要するスクランブル鍵Ks201を、ECM-Kw1000やECM-Kc1020から抽出して、端末装置102にレスポンスとして返送したりする。
- [0160] ライセンス変換処理部1216は、放送局101から受信したECMなどに含まれる情報(またはライセンスそのもの)を、蓄積コンテンツの利用を制御するためのライセンスに変換するとともに、変換したライセンスの数を管理するための部である。具体的には、ライセンス変換処理部1216は、放送局101から取得したKc伝送用ECM1100に含まれる情報を、図16に示す蓄積視聴用のライセンスのフォーマットに変換するとともに、変換したライセンスのライセンスIDと有効期限とを管理するための変換履歴であるTL1500を生成、管理する。
- [0161] ここで、ライセンス変換処理部1216が変換するライセンスの構成の一例を、図16を用いて説明する。
- [0162] ライセンス1600は、コンテンツの利用を許諾する情報であり、ライセンス識別子1601と、ライセンスID1602と、有効期限1603と、再生回数1604と、書き出し回数1605

と、コンテンツ鍵Kc1606と、ライセンス1600の改ざんを検出するための改ざん検出1607とから構成されている。

- [0163] ライセンス識別子1601は、コンテンツ配信システム1で利用可能なライセンスを識別するための識別子である。例えば、「SV-DRM LICENSE」のような識別子であり、ライセンス変換処理部1216であらかじめ保持している識別子である。
- [0164] ライセンスID1602は、コンテンツ配信システム1内でライセンスを一意に識別するための識別子である。ライセンスID1602は、Kc伝送用ECM1100のライセンスID1107の値を設定する。
- [0165] 有効期限1603は、ライセンス1600が利用可能な期間を示し、利用開始日時および利用終了日時を有する。有効期限1603は、Kc伝送用ECM1100のライセンス有効期限1108の値を設定する。
- [0166] 再生回数1604は、コンテンツを再生可能な回数を示し、再生回数が0より大である場合には、再生が可能となる。再生回数1604は、Kc伝送用ECM1100の利用可能回数1110の値を設定する。
- [0167] 書き出し回数1605は、DVD(Digital Versatile Disc)やBD(Blu-Ray Disc)などの記録媒体などへのコンテンツの複製回数を示す。書き出し回数1605は、Kc伝送用ECM1100の書き出し可能回数1111の値を設定する。
- [0168] コンテンツ鍵Kc1606は、ECM-Kc1020を復号するためのコンテンツ鍵Kc205を示す。コンテンツ鍵Kc205がバイナリ値で設定され、ECM-Kc1020を復号する場合に用いる。コンテンツ鍵Kc1606は、Kc伝送用ECM1100のコンテンツ鍵Kc1109の値を設定する。
- [0169] 改ざん検出1607は、ライセンス1600をハードディスクなどの非セキュアな領域に蓄積する場合に、改ざんの検出を行い、その正当性を確保するためのものであって、ライセンス1600の内容が更新される度に、ライセンス1600の改ざんを防止したい箇所(典型的には、ライセンス識別子1601～コンテンツ鍵Kc1606)についてハッシュ値を計算し、計算結果を管理する。このハッシュ値は、ハード的に耐タンパ化されたICカード103の内部で管理する。ハッシュアルゴリズムとしては、例えば、SHA-1(Secure Hash Algorithm 1)や、SHA-256などが挙げられる。また、ライセンス

1600をハードディスクなどの非セキュアな領域に蓄積する場合には、少なくともコンテンツ鍵Kc1606の部分は暗号化されて蓄積される。

- [0170] 以上、図16を用いて、コンテンツ配信システム1におけるライセンス1600の構成の説明を行った。
- [0171] ライセンス処理部1217は、ライセンスに基づき、コンテンツの利用可否判定をセキュアに行う。
- [0172] 具体的には、ライセンス処理部1217は、ユーザからライセンスの利用要求を受けた場合に、放送局101から取得したライセンスに含まれる利用条件に基づき、コンテンツの利用が可能かどうかを判定する。そして、利用条件がコンテンツの利用を許諾している場合に限り、ECM-Kc1020を復号するためのコンテンツ鍵Kc205をECM/EMM復号部1214に渡す、という処理を行う。
- [0173] 例えば、ライセンス処理部1217は、ライセンス1600に設定された有効期限1603を参照し、コンテンツが利用可能であるかどうかを判定する。端末装置102に保持している、図12には図示しないセキュアな計時部により提供される現在時刻を参照し、現在時刻が有効期限1603内である場合は、コンテンツの再生が可能である、というような判定処理を行う。
- [0174] 以上、図12～図16を用いて、端末装置102およびICカード103についての詳細な構成の説明を行った。
- [0175] さて、以上のように構成された端末装置102およびICカード103において、ユーザが放送局101との視聴契約を行い、放送局101の配信装置からコンテンツおよびライセンスを取得して、端末装置102に蓄積し、端末装置102においてコンテンツを利用するという一連の動作を、図17～図22に示すフローチャートを用いて説明する。
- [0176] なお、図17～図22に示すフローチャートにおいて、ユーザがPPVコンテンツを利用する場合には、コンテンツの購入処理が必要であるが、これらの処理については本発明の主眼ではないため、以下では説明を省略する。
- [0177] 最初に、端末装置102において、ユーザが放送局101と視聴契約を行う動作を、図17に示すフローチャートを用いて説明する。
- [0178] まず端末装置102において、ユーザが、ユーザI/F部1208が提供するGUIにより

、放送局101との視聴契約を行う(ステップS1701)。

- [0179] 具体的には、ユーザが、ユーザI/F部1208が提供するGUIによって、放送局101が提供するティア契約、または、PPV契約の視聴契約のうち所望の契約を選択すると、ユーザI/F部1208は、対応する契約を識別するためのID(以下、契約IDと記述)を、ICカード103のカードID1301などとともに送受信部1201に送信する。送受信部1201は、放送局101とSSL(Secure Sockets Layer)などを用いてSACを確立し、受け取った契約IDとカードID1301とを放送局101に送信する。なお、ユーザI/F部1208は、Webブラウザなどによってあらかじめ契約IDを取得済みであるものとする。また、カードID1301についても、ICカード103の挿入時などにあらかじめ取得済みであるものとする。
- [0180] 放送局101は、端末装置102からの視聴契約の申し込みを受け付ける(ステップS1702)。
- [0181] 具体的には、放送局101の通信部306は、端末装置102から契約IDなどを受信すると、契約IDを契約処理部307に渡す。
- [0182] 放送局101は、端末装置102から受信した契約IDに基づき、契約処理を行い、ユーザの契約に関する情報をデータベースに登録する(ステップS1703)。
- [0183] 具体的には、契約処理部307は、必要に応じて、クレジットカード番号や銀行口座番号などを用いて課金処理を行い、契約情報管理DB301にユーザの視聴契約情報を登録する。このとき契約処理部307は、合わせて、ICカード103固有の蓄積暗号鍵Km'305を生成し、ICカード103固有のマスタ鍵Km306とともに、契約情報管理DB301に登録する。
- [0184] なお、ICカード103毎に固有のマスタ鍵Km306については、鍵管理センタなどからあらかじめ取得しておくものとする。
- [0185] 放送局101のEMM生成部308は、視聴契約を行ったユーザに対するEMM900を生成する(ステップS1704)。
- [0186] 具体的には、EMM生成部308は、顧客管理システムなどの上位のシステムからの随時または一日一回などのEMM送出指示に基づき、契約情報管理DB301の契約情報管理テーブル400から、EMM900を送出すべきカードID401のティア契約ID

- 402～蓄積暗号鍵Km'405を抽出し、該当カードID401宛てのEMM900を生成する。EMM生成部308は、生成したEMM900をEMM暗号化部309に送信する。
- [0187] 放送局101のEMM暗号化部309は、生成したEMM900に対応するマスタ鍵で、EMM900を暗号化する(ステップS1705)。
- [0188] 具体的には、EMM暗号化部309は、EMM生成部308から受け取ったEMM900のカードID902を参照して、契約情報管理DB301の契約情報管理テーブル400から、カードID401が合致するICカード103のマスタ鍵Km406を読み出す。このマスタ鍵Km406を用いて、EMM900の必要部分をAESで暗号化する。EMM暗号化部309は、暗号化したEMM900を多重化部313に送信する。
- [0189] 放送局101は、暗号化したEMM900を、コンテンツなどと多重化し、端末装置102に送出する(ステップS1706)。
- [0190] 具体的には、多重化部313は、EMM暗号化部309から受け取ったEMM900と、コンテンツ符号化部312などから受け取ったコンテンツなどをTSパケット化した後、TS多重化する。その後、コンテンツ暗号化部314において、コンテンツの必要部分がスクランブルされ、コンテンツ送出部315が、放送波としてEMM900を含むTSを端末装置102に送出する。
- [0191] 端末装置102は、自己宛てのEMM900を受信する(ステップS1707)。
- 具体的には、端末装置102の送受信部1201および分離部1202は、事前にICカード103から取得したカードIDを用いて、受信したEMM900をフィルタリングし、自己宛てのEMM900を抽出する。
- [0192] 端末装置102の第1のカードI/F部1207は、受信したEMM900をICカード103に送出する(ステップS1708)。
- [0193] ICカード103の第2のカードI/F部1213は、端末装置102の第1のカードI/F部1207からEMM900を受信する(ステップS1709)。
- [0194] ICカード103は、ICカード103内で、EMM900に含まれる情報を管理する(ステップS1710)。
- [0195] 具体的には、第2のカードI/F部1213が受信したEMM900を、ECM/EMM復号部1214に送信する。ECM/EMM復号部1214は、EMM900のカードID902

が自身のICカード103が保持するカードIDと一致することを確認した上で、カード管理情報DB1210の共通情報テーブル1300からマスタ鍵Km1302を読み出し、EMM900のカードID902を復号する。復号後、EMM900の改ざん検出910を用いて、暗号化EMM900が正しく復号できたことを確認する。改ざんが発見された場合は、当該EMM900の処理を中断する。ECM／EMM復号部1214は、復号したEMM900をECM／EMM処理部1215に渡す。ECM／EMM処理部1215は、受け取ったEMM900を解釈し、必要な情報をカード管理情報DB1210に蓄積し、図13および図14に示した、共通情報テーブル1300および事業者別情報テーブル1400を構築する。

- [0196] なお、ここでは、端末装置102が通信ネットワーク105を通じて、放送局101に対して視聴契約の申し込みを行う場合の例を示したが、電話やハガキなどのオフラインによる視聴契約の申し込みであっても良い。
- [0197] 次に、放送局101における送出装置が、コンテンツを送出する動作を、図18に示すフローチャートを用いて説明する。
- [0198] まず、ECM生成部310は、コンテンツ送出指示を受信すると、コンテンツ送出開始に先立ち、Kc伝送用ECM1100を生成する(ステップS1801)。
- [0199] 具体的には、ECM生成部310は、番組運行管理装置などの上流システムからのコンテンツ送出指示、すなわち、ECM生成指示をトリガとして、コンテンツ単位の暗号鍵を有するKc伝送用ECM1100を生成するため、コンテンツ属性情報DB303およびコンテンツ鍵DB304を参照して、ライセンスID602、利用条件603、コンテンツ鍵Kc703などを読み出す。読み出した情報から、図11に示したKc伝送用ECM1100を生成する。ECM生成部310は、生成したKc伝送用ECM1100を、ECM暗号化部311に送信する。
- [0200] ECM暗号化部311は、ワーク鍵Kw203でKc伝送用ECM1100を暗号化する(ステップS1802)。
- [0201] 具体的には、ECM暗号化部311は、ワーク鍵DB302のワーク鍵管理テーブル500のワーク鍵利用開始日503を参照して、現在使用中のワーク鍵Kw203を特定する。特定したワーク鍵ID501とワーク鍵Kw502を読み出し、ECM生成部310から受

信したKc伝送用ECM1100の必要部分をAESでCBC+OFBモードによる暗号化を施す。合わせて、Kc伝送用ECM1100のワーク鍵ID1104に、ワーク鍵ID501を設定する。ECM暗号化部311は、暗号化したKc伝送用ECM1100を多重化部313に送信する。

- [0202] コンテンツ符号化部312は、コンテンツの読み出し、送出を開始し、コンテンツ送出中はコンテンツの送出が完了したか否かを監視する(ステップS1803)。
- [0203] 具体的には、コンテンツ符号化部312は、ステップS1801において、ECM生成部310が上流システムから受信したコンテンツ送出指示と同じ指示を受けて、コンテンツDB305のコンテンツ管理テーブル800から該当コンテンツを読み出し、コンテンツをMPEGエンコードによりコンテンツのTSを生成する。生成したTSを多重化部313に送信するとともに、コンテンツDB305からのコンテンツの読み出し、および、多重化部313へのコンテンツの送信が完了したか否かを監視する。
- [0204] ステップS1803において、NOである場合、すなわち、コンテンツの送信が完了していない場合は、ステップS1804を実行する。
- [0205] ステップS1803において、YESである場合、すなわち、コンテンツの送信が完了した場合には、本コンテンツ送出処理を終了する。
- [0206] ECM生成部310は、コンテンツの送出開始に伴い、コンテンツをスクランブルするためのスクランブル鍵Ks201を生成する(ステップS1804)。
- [0207] 具体的には、ECM生成部310は、数秒おきに更新されるスクランブル鍵Ks201を順次生成して、生成したスクランブル鍵Ks201をコンテンツ暗号化部314に逐次送信する処理を行う。
- [0208] ECM生成部310は、コンテンツ属性情報からECMを生成する(ステップS1805)。
- [0209] 具体的には、コンテンツの送出に合わせて、コンテンツ属性情報DB303のコンテンツ属性情報管理テーブル600の契約情報604などを読み出し、ECM-Kw1000、ECM-Kc1020を生成する。ECM生成部310は、生成したECM-Kw1000、ECM-Kc1020を、ECM暗号化部311に送信する。
- [0210] ECM暗号化部311は、ワーク鍵Kw203でECM-Kwを暗号化する(ステップS1

806)。

- [0211] 具体的には、ECM暗号化部311は、ワーク鍵Kw203によるKc伝送用ECM1100の暗号化と同様の方法で、ワーク鍵DB302のワーク鍵管理テーブル500のワーク鍵利用開始日503を参照して、現在使用中のワーク鍵Kw203を特定し、ワーク鍵Kw502でECM-Kw1000をAESで暗号化する。ECM暗号化部311は、暗号化したECM-Kw1000を多重化部313に送信する。
- [0212] ECM暗号化部311は、コンテンツ鍵Kc205でECM-Kcを暗号化する(ステップS1806)。
- [0213] 具体的には、ECM暗号化部311は、コンテンツ鍵DB304のコンテンツ鍵管理テーブル700を参照して、送出するコンテンツとコンテンツID701およびライセンス702が一致するレコードのコンテンツ鍵Kc703を読み出す。ここで、送出するコンテンツのコンテンツIDとライセンスIDは、上流システムからのコンテンツ送出指示の際に、上流システムなどから取得済みであるとする。読み出したコンテンツ鍵Kc703を用いて、ECM生成部310から受信したKc伝送用ECM1100の必要部分をAESでCBC+OFBモードによる暗号化を施す。ECM暗号化部311は、暗号化したECM-Kc1020を多重化部313に送信する。
- [0214] コンテンツ暗号化部314は、コンテンツやECMが多重化されたTSをスクランブルする(ステップS1808)。
- [0215] 具体的には、コンテンツ暗号化部314は、多重化部313においてコンテンツのTSやECM-Kw1000、ECM-Kc1020、Kc伝送用ECM1100などのTSを多重化したTSのうち、映像、音声、データなどのコンテンツのTSパケットを選択して、AESのCBC+OFBモードでTSパケットのペイロード部分をスクランブルする。
- [0216] コンテンツ送出部315は、暗号化されたTSを送出する(ステップS1809)。
 具体的には、コンテンツ送出部315は、コンテンツ暗号化部314においてスクランブルされたTSを、放送波として端末装置102に送出する。
- [0217] なお、ここでは、コンテンツの送出開始に合わせて、スクランブル鍵Ks201、すなわち、ECM-Kw1000、ECM-Kc1020の送出を行う場合の例を示したが、端末装置102において、コンテンツの先頭から確実にデスクランブル可能となるように、コン

テンツの送出開始に先立ってECM-Kw1000、ECM-Kc1020を多重、送出することが望ましい。

- [0218] 以上、図18を用いて、放送局101によるコンテンツの送出処理についての詳細な説明を終了する。
- [0219] 次に、端末装置102が、デジタル放送104からコンテンツを受信し、蓄積部1203に蓄積する動作を、図19～図21に示すフローチャート等を用いて説明する。
- [0220] 図19は、端末装置102およびICカード103におけるコンテンツ受信およびライセンス変換処理を示すフローチャートである。ただし、本処理において、ICカード103におけるライセンス変換可否判定処理については、別途、図21に示すフローチャートを用いて説明する。
- [0221] まず、端末装置102における蓄積管理部1204は、蓄積部1203に蓄積するコンテンツの蓄積状況を監視し、コンテンツ蓄積が終了しているか否かを確認する(ステップS1901)。
- [0222] 具体的には、蓄積管理部1204は、ユーザから指定されたサーバ型放送TypeIコンテンツをチューニングし、パーシャルTSとして蓄積部1203に順次蓄積する。蓄積処理の間、PSI/SI(Program Specific Information/Service Information)などを参照しながら、当該コンテンツを蓄積完了したか否かを監視する。
- [0223] ステップS1901において、YESである場合、すなわち、コンテンツの蓄積が未完了である場合には、ステップS1902を実行する。
- [0224] ステップS1901において、NOである場合、すなわち、コンテンツの蓄積が完了した場合には、本コンテンツ蓄積処理を終了する。
- [0225] 分離部1202は、Kc伝送用ECM1100を取得したか否かを判断する(ステップS1902)。
- [0226] 具体的には、分離部1202は、受信したTSのPAT、PMTなどを参照し、Kc伝送用ECMのPIDが付与されたTSパケットからKc伝送用ECM1100を再構成するが、1つのコンテンツ蓄積において、少なくとも1回取得すれば良いKc伝送用ECM1100を取得したか否かを監視する。
- [0227] ステップS1902において、YESである場合、すなわち、Kc伝送用ECM1100を未

取得である場合には、ステップS1903を実行する。

- [0228] ステップS1902において、NOである場合、すなわち、Kc伝送用ECM1100を取得済みである場合には、ステップS1912を実行する。
- [0229] 分離部1202は、Kc伝送用ECMを分離し、ICカード103に送信する(ステップS1903)。
- [0230] 具体的には、分離部1202は、ステップS1902の処理において再構成したKc伝送用ECM1100を取得して、第1のカードI/F部1207を通じて、ICカード103に送信する。
- [0231] ICカード103は、受信したKc伝送用ECM1100を変換しても良いか否かを判定する(ステップS1904)。
- [0232] 具体的には、ICカード103の第2のカードI/F部1213は、端末装置102の第1のカードI/F部1207が送信した、暗号化されたKc伝送用ECM1100を受信し、暗号復号処理の後、ライセンス変換処理部1216は、ICカード103内部に蓄積した変換履歴DB1211を用いて、ライセンス変換処理を行ってもよいか否かの判定処理を実行する。なお、本ライセンス変換可否判定処理の詳細については、後で図21を用いて説明するので、ここでは詳細な説明は行わない。
- [0233] ICカード103のライセンス変換処理部1216は、ライセンス変換可否判定処理の結果、ライセンス変換が許可されているか否かを確認する(ステップS1905)。
- [0234] ステップS1905において、YESである場合、すなわち、ライセンス変換が許可されている場合には、ステップS1906を実行する。
- [0235] ステップS1905において、NOである場合、すなわち、ライセンス変換が許可されていない場合には、ステップS1910を実行する。
- [0236] ライセンス変換処理部1216は、Kc伝送用ECM1100をライセンス変換し、蓄積視聴用のライセンス1600を生成する(ステップS1906)。
- [0237] 具体的には、ライセンス変換処理部1216は、Kc伝送用ECM1100に含まれるライセンスID1107、ライセンス有効期限1108などを取得して、図16に示すようなライセンス1600を生成する。
- [0238] ライセンス変換処理部1216は、変換したライセンスがティアコンテンツであるか、P

PVコンテンツであるかを判定する(ステップS1907)。

- [0239] 具体的には、ライセンス変換処理部1216は、Kc伝送用ECM1100のサービスタイプ1103を参照して、サービスタイプ1103が「TEIRCONT」(ティアコンテンツ)であるか、「PPVCONT」(PPVコンテンツ)であるかを判断する。
- [0240] ステップS1907において、YESである場合、すなわち、ティアコンテンツである場合には、ステップS1908を実行する。
- [0241] ステップS1907において、NOである場合、すなわち、PPVコンテンツである場合には、ライセンス変換履歴を記録する必要がないので、ステップS1908を実行せず、ステップS1909を実行する。ただし、PPVコンテンツのライセンス1600は、購入処理を経て初めて利用可能になるライセンスであるので、例えば、ライセンス変換直後には、ライセンス1600と合わせて、当該ライセンスが未購入であることを示すフラグを保持するようにし、購入処理後にフラグを削除することにより、当該ライセンスが購入済みであることを示す、といった処理が必要である。
- [0242] ライセンス変換処理部1216は、当該ライセンスの変換履歴を記録する(ステップS1908)。
- [0243] 具体的には、ライセンス変換処理部1216は、変換履歴DB1211に蓄積されているTL1500のライセンスID1501とライセンス変換期限1502に、Kc伝送用ECM1100のライセンスID1107とライセンス変換期限1106を追加する。
- [0244] ライセンス処理部1217は、変換したライセンスをライセンスDB1212に蓄積する(ステップS1909)。
- [0245] 第2のカードI/F部1213は、端末装置102に対して、Kc伝送用ECM1100によるライセンス変換要求に対するレスポンスを送信する(ステップS1910)。
- [0246] 具体的には、第2のカードI/F部1213は、当該コンテンツのライセンス変換が許可されており、ライセンス変換が完了したか、あるいは、当該コンテンツのライセンス変換が許可されていない、または、ライセンス変換に失敗した、などのレスポンスメッセージを生成して、端末装置102に送信する。
- [0247] なお、ステップS1905において、NOである場合のように、当該コンテンツのライセンス変換が許可されていない場合には、図20に示すようなメッセージをユーザに提

示する。

- [0248] 図20は、ユーザI/F部1208がユーザに提示するウォーニングメッセージの一例を示す図である。モニタ2001に表示されているメッセージ2002は、ユーザがICカード103において、コンテンツ「マンデースポーツ」のライセンスIDに対応するライセンスを既にライセンス変換し、取得しているため、これ以上は取得できない旨を示している。
- [0249] 第1のカードI/F部1207は、ICカード103からのレスポンスを受信する(ステップS1911)。
- [0250] 具体的には、第1のカードI/F部1207は、ICカード103の第2のカードI/F部1213から、Kc伝送用ECM1100の送信に対するライセンス変換結果のレスポンスを受信する。
- [0251] 端末装置102の蓄積管理部1204は、コンテンツを蓄積部1203に蓄積する処理を行う(ステップS1912)。
- [0252] 具体的には、蓄積管理部1204は、コンテンツ、ECM-Kc1020、Kc伝送用ECM1100などのTSパケットを、順次蓄積部1203に蓄積するとともに、合わせて、PMTなどから生成したSIT、DITも蓄積する。なお、何らかの原因によりICカード103でのライセンス変換処理に失敗した場合でも、後で再度ライセンス変換を試みることができるように、コンテンツやECM-Kc1020、Kc伝送用ECM1100の蓄積処理は継続する。
- [0253] 以上、図19を用いて、端末装置102におけるコンテンツ蓄積処理についての説明を行った。
- [0254] 次に、ICカード103でのライセンス変換可否判定処理について、図21を用いて詳細に説明する。
- [0255] まず、ICカードのECM/EMM復号部1214は、カード管理情報DB1210を参照して、Kc伝送用ECM1100を復号するためのワーク鍵Kw203が存在するか否かを判定する(ステップS2101)。
- [0256] 具体的には、ECM/EMM復号部1214は、カード管理情報DB1210の事業者別情報テーブル1400を参照して、Kc伝送用ECM1100の事業者ID1102と、事業

者ID1401が一致する事業者IDのレコードを検索して、ワーク鍵Kw1406を読み出す。このとき、端末装置102からKc伝送用ECM1100と一緒に取得した現在時刻が、有効期限1404を超過していたり、Kc伝送用ECM1100のワーク鍵ID1104と事業者別情報テーブル1400のワーク鍵ID1405が一致しない場合などには、ワーク鍵Kw203が存在しないものとして処理する。

- [0257] ステップS2101において、YESである場合、すなわち、ワーク鍵Kw1406が存在する場合には、ステップS2102を実行する。
- [0258] ステップS2101において、NOである場合、すなわち、ワーク鍵Kw1406が存在しない場合には、ステップS2111を実行する。
- [0259] ECM／EMM復号部1214は、ワーク鍵Kw1406でKc伝送用ECM1100を復号する(ステップS2102)。
- [0260] 具体的には、ECM／EMM復号部1214は、ステップS2101で取得したワーク鍵Kw1406で、AESによりKc伝送用ECM1100の暗号化部を復号し、Kc伝送用ECM1100の改ざん検出1110により、Kc伝送用ECM1100が改ざんされていないかを確認する。万一、Kc伝送用ECM1100が改ざんされていることが検出された場合には、ライセンス変換は許可できないので、ステップS2111を実行して、本処理を終了する(図21には図示せず)。
- [0261] ECM／EMM処理部1215は、ICカード103が、当該コンテンツを視聴するための契約を有しているか否かを判定する(ステップS2103)。
- [0262] 具体的には、ECM／EMM処理部1215は、Kc伝送用ECM1100の契約判定情報1105と、カード管理情報DB1210の事業者別情報テーブル1400のティア契約ID1402またはPPV契約ID1403を比較して、いずれかのIDが一致するか否かの判定処理を行う。
- [0263] ステップS2103において、YESである場合、すなわち、いずれかのIDが一致する場合には、ステップS2104を実行する。
- [0264] ステップS2103において、NOである場合、すなわち、いずれのIDも一致しない場合には、ステップS2111を実行する。
- [0265] ライセンス変換処理部1216は、Kc伝送用ECM1100がライセンス変換の期限内

であるかどうかを判定する(ステップS2104)。

- [0266] 具体的には、ライセンス変換処理部1216は、Kc伝送用ECM1100のライセンス変換期限1106を参照して、端末装置102からKc伝送用ECM1100と一緒に取得した現在時刻と比較することにより、当該Kc伝送用ECM1100がライセンス変換期限内であるか否かを判定する。
- [0267] ステップS2104において、YESである場合、すなわち、ライセンス変換期限1106が現在時刻よりも新である場合には、ライセンス変換期限内であると判定し、ステップS2105を実行する。
- [0268] ステップS2104において、NOである場合、すなわち、ライセンス変換期限1106が現在時刻よりも旧である場合には、ライセンス変換期限外であると判定し、ステップS2111を実行する。
- [0269] ライセンス変換処理部1216は、変換履歴DB1211を参照して、該当ライセンスIDの変換履歴を検索する(ステップS2105)。
- [0270] 具体的には、ライセンス変換処理部1216は、変換履歴DB1211のTL1500を参照し、Kc伝送用ECM1100のライセンスID1107と一致するライセンスID1501のレコードを検索する。
- [0271] ライセンス変換処理部1216は、該当ライセンスIDの変換履歴が存在するか否かを判定する(ステップS2106)。
- [0272] 具体的には、ライセンス変換処理部1216は、ステップS2105の検索結果を参照し、Kc伝送用ECM1100のライセンスID1107とTL1500のライセンスID1501が一致するレコードが存在するか否かを確認する。
- [0273] ステップS2106において、YESである場合、すなわち、該当ライセンスIDの変換履歴が存在しない場合には、ステップS2107を実行する。
- [0274] ステップS2106において、NOである場合、すなわち、該当ライセンスIDの変換履歴が存在する場合には、ステップS2111を実行する。
- [0275] ライセンス変換処理部1216は、TL1500に空きレコードまたは有効期限を超過したレコードが存在するか否かを検索する(ステップS2107)。
- [0276] 具体的には、ライセンス変換処理部1216は、新たにライセンス変換を行うライセン

スIDを追記するレコードを発見するため、TL1500を参照して、空きレコードを検索する。空きレコードが存在しない場合は、TL1500の、ライセンス変換期限1502と、端末装置102からKc伝送用ECM1100と一緒に取得した現在時刻を比較し、ライセンス変換期限1502が現在時刻より新であるレコードを検索する。

- [0277] ライセンス変換処理部1216は、変換履歴DB1211に空きレコードもしくはライセンス変換期限を超過しているレコードが存在するか否かを判定する(ステップS2108)。
- [0278] 具体的には、ライセンス変換処理部1216は、ステップS2107の検索結果を参照し、TL1500に空きレコードをもしくはライセンス変換期限1502を超過しているレコードが存在するか否かを判定する。
- [0279] ステップS2108において、YESである場合、すなわち、空きレコードまたはライセンス変換期限1502を超過しているレコードが存在する場合には、ステップS2109を実行する。
- [0280] ステップS2108において、NOである場合、すなわち、空きレコードまたはライセンス変換期限1502を超過しているレコードが存在しない場合には、これ以上ライセンス変換を実行することはできないため、ステップS2111を実行する。
- [0281] ライセンス変換処理部1216は、ステップS2108で判定した結果に基づき、空きレコードがない場合には、ライセンス変換期限1502を超過したレコードを削除し、新たなライセンスID1501の追加をできるようにする(ステップS2109)。
- [0282] ライセンス変換処理部1216は、当該Kc伝送用ECM1100のライセンスを変換を許可と判定し、本ライセンス変換可否判定処理を終了する(ステップS2110)。
- [0283] ライセンス変換処理部1216は、当該Kc伝送用ECM1100のライセンスを変換は不許可と判定し、本ライセンス変換可否判定処理を終了する(ステップS2111)。
- [0284] 以上、図19～図21を用いて、コンテンツ蓄積時の端末装置102およびICカード103の処理の詳細について説明を行った。
- [0285] 最後に、端末装置102が、蓄積部1203のコンテンツを蓄積視聴する動作を、図22に示すフローチャートを用いて説明する。
- [0286] まず、ユーザが視聴したい蓄積コンテンツのライセンスIDを指定すると、端末装置102は、ICカード103に対してコンテンツ鍵を要求する(ステップS2201)。

- [0287] 具体的には、端末装置102のユーザI/F部1208は、メタデータなどを利用して、ユーザが再生したいコンテンツのライセンスIDを取得し、ライセンスIDをICカード103に送信するため、第1のカードI/F部1207に送信する。第1のカードI/F部1207は、受信したライセンスIDをICカード103に送信する。
- [0288] ICカード103は、ライセンスDB1212から該当ライセンスIDを有するライセンスを検索する(ステップS2202)。
- [0289] 具体的には、ICカード103の第2のカードI/F部1213は、受信したライセンスIDをライセンス処理部1217に送信し、ライセンス処理部1217はライセンスIDをキーとして、ライセンスDB1212を検索する。
- [0290] ライセンス処理部1217は、要求されたライセンスIDと一致する、有効なライセンスが存在するか否かを判定する(ステップS2203)。
- [0291] ステップS2203において、YESである場合、すなわち、有効なライセンスが存在する場合には、ステップS2204を実行する。
- [0292] ステップS2203において、NOである場合、すなわち、有効なライセンスが存在しない場合には、再生不可として、ステップS2205を実行する。
- [0293] ライセンス処理部1217は、取得したライセンスからコンテンツ鍵と利用条件を取得する(ステップS2204)。
- [0294] 具体的には、ライセンス処理部1217は、取得したライセンス1600から、コンテンツ鍵Kc1606と、有効期限1603、再生回数1604、書き出し回数1605を取得する。まず、有効期限1603～書き出し回数1605のコンテンツの利用条件については、ライセンス処理部1217において、有効期限1603と現在時刻との比較により、ライセンスが有効であるか否かを判定する。同様に、再生回数1604および書き出し回数1605については、ここではユーザがコンテンツの再生を要求していることから、再生回数1604を参照し、再生回数1604が0より大であるか否かを判定する。この利用条件判定において、コンテンツ利用可と判定された場合には、ライセンス処理部1217は、コンテンツ再生と同期して端末装置102から受け取る暗号化ECM-Kc1020を復号するため、コンテンツ鍵Kc1606をECM/EMM復号部1214に送信する。コンテンツ鍵Kc1606は、当該コンテンツの再生の間は、ECM/EMM復号部1214におい

て保持される。

- [0295] 第2のカードI/F部1213は、端末装置102に対して、ライセンス処理結果のレスポンスを送信する(ステップS2205)。
- [0296] 具体的には、第2のカードI/F部1213は、ライセンス処理部1217による当該ライセンスの検索、および、ライセンスの利用可否判定の結果を取得して、端末装置102の第1のカードI/F部1207に対して、レスポンスとしてその旨を送信する。
- [0297] 端末装置102の第1のカードI/F部1207は、ICカード103からのレスポンスを受信して、コンテンツ復号部1205に送信し、コンテンツ復号部1205は当該コンテンツが再生可能かどうかを確認する(ステップS2206)。
- [0298] ステップS2206において、YESである場合、すなわち、コンテンツが再生可能である場合には、ステップS2207を実行する。
- [0299] ステップS2206において、NOである場合、すなわち、コンテンツが再生不可である場合には、本コンテンツ利用処理を終了する。
- [0300] 蓄積管理部1204は、蓄積部1203から該当コンテンツを読み出し、コンテンツ復号部1205およびコンテンツ利用部1206が暗号化コンテンツの復号、および、コンテンツのデコードを開始する(ステップS2207)。
- [0301] 蓄積管理部1204は、蓄積部1203から該当コンテンツの全TSパケットを読み出し、コンテンツの再生が終了したか否かを判定する(ステップS2208)。
- [0302] ステップS2208において、NOである場合、すなわち、コンテンツの再生が継続中である場合には、ステップS2209を実行する。
- [0303] ステップS2208において、YESである場合、すなわち、コンテンツの再生が終了した場合には、本コンテンツ再生処理を終了する。
- [0304] 分離部1202は、蓄積管理部1204が読み出した該当コンテンツからECM-Kc1020を受け取り、ICカード103に送信する(ステップS2209)。
- [0305] 具体的には、分離部1202は、該当コンテンツからECM-Kc1020のPIDのTSパケットを取得し、ECM-Kc1020を再構成する。再構成したECM-Kc1020を、第1のカードI/F部に渡し、第1のカードI/F部1207がICカード103にECM-Kc1020を送信する。なお、ECM-Kc1020に含まれるスクランブル鍵Ks201は数秒お

きに更新されるため、本ステップの処理は数秒に1回の割合で行う必要がある。

- [0306] ICカード103は、コンテンツ鍵Kc205によって受信したECM-Kc1020を復号する(ステップS2211)。
- [0307] 具体的には、ICカード103の第2のカードI/F部1213が端末装置102の第1のカードI/F部1207から受信したECM-Kc1020を、ECM/EMM復号部1214に送信し、ECM/EMM復号部1214は、保持しているコンテンツ鍵Kc1606でECM-Kc1020を復号する。
- [0308] ICカード103は、ECM-Kc1020から取得したスクランブル鍵Kc201を端末装置102に送信する(ステップS2212)。
- [0309] 具体的には、ICカード103のECM/EMM処理部1215は、復号したECM-Kc1020からスクランブル鍵Ks201を取得し、第2のカードI/F部1213を通じて、端末装置102にスクランブル鍵Ks201を送信する。なお、この際に、ライセンス1600に設定されたコンテンツの利用条件を参照して、スクランブル鍵Kc201を端末装置102に送信するか否かを判定するようにしても良い。
- [0310] 端末装置102のコンテンツ復号部1205は、ICカード103から取得したスクランブル鍵Ks201で、コンテンツをデスクランブルし、コンテンツ利用部1206がコンテンツをデコードする(ステップS2210)。
- [0311] 具体的には、コンテンツ復号部1205は、第1のカードI/F部1207から、ICカード103より取得したスクランブル鍵Ks201を逐次受け取り、コンテンツ復号部1205に設定する。蓄積部103から読み出したコンテンツの暗号化TS packetsを、スクランブル鍵Ks201を用いてデスクランブルし、コンテンツ利用部1206に送信する。コンテンツ利用部1206は、コンテンツ復号部1205から受信したデスクランブル後のコンテンツをMPEGデコードし、図示しないモニタなどに出力する。
- [0312] なお、端末装置102のコンテンツ復号部1205やコンテンツ利用部1206、あるいは、ICカード103のECM/EMM復号部1214などにおいて利用条件に基づき、有効期間、累積の利用時間などのコンテンツの利用制御を行うようにしても良い。この場合、ライセンス1600には、対応した利用条件が含まれるものとする。
- [0313] 以上、図22を用いて、端末装置102およびICカード103におけるコンテンツ利用

処理について説明した。

- [0314] 以上のように、コンテンツ配信システム1に適用したデジタル権利管理システムでは、端末装置で取得したライセンスのIDと有効期限とを、ライセンスの取得履歴として管理し、少なくともライセンスの取得期限までライセンス取得履歴を保持しておくようにしている。そのため、無制限なライセンス取得の防止と、管理するデータサイズの増大の防止とを両立することでき、事業者の権利を十分保護することが可能となる。
- [0315] なお、本発明における実施の形態では、サーバ型放送方式のKc伝送用ECM1100を用いて、放送局101の送出装置から端末装置102およびICカード103に対して、ライセンス1600に設定する情報を配信するようにしたが、これに限られるものではなく、サーバ型放送方式のECM-Kw1000、ECM-Kc1020、EMM900をはじめ、Kc配信用EMMやサーバ型放送方式のTypeIIで用いられるACI(Account Control Information)などに設定するようにしても良い。また、ライセンス1600に設定する情報を配信するのに加え、ライセンス1600とは異なるフォーマットのライセンスを含めて配信するようにしても良いし、ECMやEMMをライセンス1600とは異なるフォーマットのライセンスであるとも考えることもできる。
- [0316] また、本発明における実施の形態では、ライセンス1600をICカード103内部に蓄積するようにしたが、ICカード103の記憶容量が大きくない場合を考慮して、少なくともライセンス1600の一部を端末装置102に蓄積するようにしても良い。
- [0317] この場合、ライセンス変換により生成したライセンス1600のセキュリティを確保するために、暗号化が必要である。この暗号化においては、例えば、ICカード103固有のマスタ鍵Km252や複数の端末装置102であらかじめ共有している暗号鍵(グループ鍵)、あるいは、図13で示した蓄積暗号鍵Km'1303など、配信時のワーク鍵Kw203とは異なる暗号鍵を用いることにより、ライセンス1600を端末装置102、ICカード103や、これらの集合にバインドするようにしても良い。
- [0318] あるいは、ライセンス変換前のKc伝送用ECM1100などを端末装置102の蓄積部1203にそのまま蓄積するようにしても良い。この際、暗号変換を行わずにそのまま蓄積しても良いし、ワーク鍵Kw203の定期的または不定期の更新に備えるため、ライセンス1600と同様、Kc伝送用ECMの暗号変換を行うようにしても良い。なお、端末

装置102およびICカード103において、ライセンスの暗号変換処理を行う場合には、図23に示すように、ICカード103の内部にECM/EMM再暗号化部2301を追加すると良い。

[0319] また、本発明における実施の形態では、ライセンス変換履歴であるTL1500において、ライセンスID1501を用いて、ライセンス変換を制御する場合の例を示したが、図24に示すように、Kc伝送用ECM2400にECMを識別するためのID(ECM-ID2401)を設けるようにしても良い。この場合、TL1500において、ライセンスID1501に代えて、ECM-ID2401を用いて、ライセンス変換を制御することができる。ただし、ライセンス1600単位のライセンス変換制御ではなく、Kc伝送用ECM1100単位のライセンス変換制御となる。あるいは、TL1500において、ライセンスID1501に加えて、ECM-ID2401を合わせて用いることにより、ライセンス変換を制御するようにしても良い。この場合、異なるKc伝送用ECM1100に同一ライセンスIDのライセンス1600が含まれるような場合(すなわち、異なるサービスから同一ライセンスを得る場合)や、通信ネットワーク105などから同一ライセンスIDのライセンス1600を取得した場合でも、ライセンス1600を取得した先を区別することができるため、異なるサービスから同一ライセンスを取得したい場合などにおいて、ライセンス変換ができないといった問題を解決することができる。さらに、これらのIDは、ライセンスやKc伝送用ECM1100などを識別可能な情報であればこれに限られるものではないので、ライセンスのハッシュ値、MAC、URIなどを用いるようにしても良い。

[0320] また、本発明における実施の形態では、Kc伝送用ECM1100のライセンス変換期限1106(TL1500のライセンス変換期限1502)を絶対日時で表現したが、相対日時を設定するようにしても良い。例えば、ライセンス有効期限1108からの相対日時としても良いし、端末装置102でKc伝送用ECM1100を受信した日時からの相対日時などとしても良い。また、変換が許可される終了日時のみである場合の例を示したが、合わせて開始日時を付与するようにしても良い。

[0321] また、本発明における実施の形態では、ライセンス1600には必ず有効期限1603が設定される場合の例を示したが、図24で示したKc伝送用ECM2400のように、有効期限1603(Kc伝送用ECM2400のライセンス有効期限1108)が無期限であり、

Kc伝送用ECM2400にライセンス変換期限が設定されていない場合も考えられる。この場合には、ICカード103のライセンス変換処理部1216がTL1500のライセンス変換期限1502を生成するようにしても良い。ライセンス変換期限1502の生成にあたっては、Kc伝送用ECM2400の受信日時やライセンス変換を行った日時に一定の期間(例えば、1ヶ月など)を加算するという方法などが考えられる。この加算値については、システム固定値として、端末装置102やICカード103で保持しておく方法もあるが、デジタル放送104や通信ネットワーク105などで、放送局101から動的に変更できるようにしても良い。

[0322] また、本発明における実施の形態では、TL1500には、ライセンスID1501およびライセンス変換期限1502を記載する場合の例を示したが、図25に示すように、TL2500として、事業者ID2501、サービスタイプ2503、購入情報2504、取得ライセンス数2506を合わせて記載するようにしても良い。これによれば、事業者ID2501を記載するようにしているので、ライセンス2502を事業者毎にユニークな値とすることができる。また、サービスタイプ2503を記載するようにしているので、ティアコンテンツに関するライセンス変換履歴に加えて、PPVコンテンツに関するライセンス変換履歴も統合して管理することが可能となる。また、購入情報2504として、PPVコンテンツを購入した日時を合わせて記載するようにしている。また、取得ライセンス数2506を記載するようにしているので、あらかじめシステム固定値として設定されていたり、放送局101からKc伝送用ECM1100などによって、1つのライセンスに関してユーザが取得可能なライセンス数(すなわち、コピー可能なライセンス数)が指定されたりする場合には、取得ライセンス数2506を記録することによって、取得可能なライセンス数を確実に制御することが可能となる。また、取得可能なライセンス数に限らず、それ以外のライセンスの取得に関する条件を管理するようにしても良い。

[0323] なお、上記で説明したTL2500を用いる場合、サービスタイプ2503、購入情報2504を用いて、同一のPPVコンテンツ(PPVライセンス)を再度購入する場合に、図26に示すようなメッセージをユーザに提示することができる。

[0324] 図26は、ユーザI/F部1208がユーザに提示するウォーニングメッセージの一例を示す図である。モニタ2601に表示されているメッセージ2602は、ユーザがコンテン

ツ「神器2」のライセンスを2004/4/15 19:00:00に購入済であるので、同一コンテンツを再購入してもよいか否かをユーザに確認する旨のメッセージを示している。

[0325] なお、本発明における実施の形態では、ICカード103で、最初にライセンス変換処理を行った端末装置102の端末装置IDを記録しておくことにより、端末装置102とICカード103とをバインドする場合の例を示したが、これに限られるものでなく、コンテンツやライセンスを共有可能な複数の端末装置102およびICカード103からなるドメインと呼ばれる集合を識別するためのドメインIDを、端末装置IDに代えて用いるようにしても良い。

[0326] また、本発明における実施の形態では、TL1500において、必ずライセンス変換期限1502を管理する場合の例を示したが、Kc伝送用ECM1100にライセンス変換期限1106やライセンス有効期限1108が設定されていないライセンスのライセンス変換履歴に関しては、時限で管理するのではなく、TL1500のレコード数などにより管理し、古いレコードから消去するなど、ハイブリッドな構成とするようにしても良い。

[0327] また、本発明における実施の形態では、Kc伝送用ECM1100のサービスタイプ1103を参照して、TL1500にライセンス変換履歴のレコードを追加するか否かを決定するようにしたが、Kc伝送用ECM1100に設定されたコンテンツの利用条件(ライセンス有効期限1108、利用可能回数1110、書き出し可能回数1111などがあげられるが、これらに限られるものではない)がステートを有するか否かによって、レコードを追加するか否かを決定するようにしても良い。このため、Kc伝送用ECM1100またはライセンス1600に、ステートを有するライセンスであるか否かの識別情報を設けても良い。例えば、利用条件がステートを有するライセンスのみレコードとして追加し、ステートを有さないライセンスはレコードとして追加しない、などの方法が考えられる。ここで、利用条件がステートを有するとは、主として利用可能回数1110、書き出し可能回数1111などの回数制限の利用条件などがあげられ、ステートを有さない利用条件としては、主として有効期限1108などがあげられる。

[0328] また、本発明における実施の形態では、TL1500において、新たなライセンス変換履歴のレコードを追加する際に、ライセンス変換期限1502が経過したレコードを削除するようにしたが、定期的にライセンス変換期限1502が経過したレコードを検索し

て、削除したり、ICカード103が端末装置102から特定のコマンドを受信した場合に、ライセンス変換期限1502が経過したレコードを検索して、削除したりするようにしても良い。また、ライセンス変換期限1502が経過したレコードの削除のための条件を、放送局101から動的に更新できるようにしても良い。さらに、ユーザ指示によって削除させるようにしても良い。

- [0329] また、本発明における実施の形態では、ICカード103の内部でTL1500を管理するようにしたが、ICカード103の記憶容量を考慮して、少なくともTL1500の一部を端末装置102の蓄積部1203において保持するようにしても良い。このとき、蓄積部1203において、悪意あるユーザなどによるTL1500の不正な操作を防止するため、蓄積部1203に保持するTL1500のハッシュ値を、ICカード103で保持する必要がある。また、この場合、ある端末装置102の蓄積部1203にTL1500を蓄積した場合、他の端末装置102で新たにライセンス取得(変換)を行うと、ユーザが取得可能なライセンス数の不整合が生ずる可能性がある。よって、端末装置102にTL1500を蓄積した場合には、当該端末装置102を一意に識別するIDをICカード103で保持することにより、ライセンスを取得可能な端末装置102を限定する必要がある。また、事前にこのような問題を回避するため、最初にライセンスを取得した端末装置102のIDをICカード103で保持しておくことによって、あらかじめライセンスを取得可能な端末装置102を限定するようにしても良い。

- [0330] なお、上記のように、ライセンスを取得可能な端末装置102を限定する場合、図27に示すように、「別端末で既にライセンスを取得しているため、この端末ではライセンスは取得できません。」などのメッセージ(2702)をユーザに提示するようにしても良い。合わせて、ライセンスを取得可能な端末の識別子(図27では、TERMINAL-ID-1)を提示するようにしても良い。また、これに限らず、他のカードにライセンスを移動した場合などにメッセージをユーザに提示するようにしても良い。

- [0331] また、本発明における実施の形態では、ICカード103単位でTL1500を管理するようにしたが、ICカード103内部で放送局101(事業者)毎に管理するようにしても良い。また、複数のICカード103間で連携することにより、複数ICカード103(ドメイン)毎で管理するようにしても良い。

- [0332] また、ライセンス変換履歴であるTL1500を、放送局101や他の端末装置102、他のICカード103に送信し、放送局101や他の端末装置102、他のICカード103で利用することもできる。
- [0333] また、ICカード103でのライセンス変換処理中において、端末装置102の電源断や、ICカードの取り外しなどにより、ライセンス変換完了前にTL1500のみが残ってしまい、ユーザが不利益を被る場合に備えて、ICカード103で一定の回数に限って再取得を許可するようにしたり、通信ネットワーク105を用いて、放送局101と通信を行い、TL1500を参照しつつ、ライセンス1600を再取得できるようにしたりすることもできる。
- [0334] また、本発明における実施の形態では、放送局101における送出装置、端末装置102を機能ブロックで構成することとしたが、図17～図22に示したフローチャートを実現するプログラムをCPU、記憶装置、通信装置などからなる汎用のコンピュータ装置で実行することによって、放送局101における送出装置や、端末装置102を実現するようにしてもよい。
- [0335] また、配信装置および端末装置を構成する各機能ブロックは、複数のシステムLSIなどで実現してもよいし、単一のシステムLSIで実現してもよい。
- [0336] さらに、本発明における実施の形態では、単一の配信経路からコンテンツやライセンス、制御情報などを取得する場合の例を示したが、デジタル放送とインターネットを併用したり、パッケージメディアとインターネットを併用したりといった、複合的な配信経路から構成されたコンテンツ配信システムに適用することもできる。
- [0337] (実施の形態2)

以下、本発明に係るデジタル権利管理システムの第二の実施の形態について図面を参照しながら説明を行う。尚、上述した実施の形態1においては、ライセンスIDとライセンス変換期限を用いて受信装置側でライセンスの変換処理における管理を行うが、ユーザが実際にコンテンツを視聴するか否かに関わらず、ライセンスをICカードに取り込むために、小メモリ容量のICカードの容量を圧迫してしまうという問題がある。これは、月極め契約等であるティア契約の場合には現実的な問題となり、また、上述したように、受信装置に取り込んだ後のライセンスをICカードでなく端末装置に記

録しておく場合でも、ライセンスの改ざん防止等のため、ICカードでライセンスのハッシュ値を記録、管理する必要があり、大量のライセンス管理は困難であるという問題が生じる。

- [0338] 本実施の形態2に係るデジタル権利管理システムにおいては、これらの課題を解決すべく、ライセンスに付与されている暗号変換期限を用いて、ユーザが実際に使用するライセンスのみをICカードに取り込むことにより、ICカードのライセンス管理におけるデータ量を軽減すると共に、ライセンスの不正使用をも防止することが可能なデジタル権利管理システムを提供する。
- [0339] 図28は、本実施の形態2に係る放送局101の機能ブロック図を示す。本実施の形態2においては、放送局101のECM生成部2801はKc伝送用ECMへの暗号変換期限の付与を行う。尚、他の処理部の機能は上述の実施の形態1と同様であるためにその説明を省略する。
- [0340] 図29は、本実施の形態2に係る送出装置のコンテンツ属性情報DB303に記録されているコンテンツ属性情報管理テーブル2900の一例を示す図である。
- [0341] このコンテンツ属性情報管理テーブル2900には、コンテンツID2901、ライセンスID2902、利用条件2903、契約情報2904に加えて、受信装置側における再暗号化期限となる暗号変換期限2905が付与されている。受信装置では、この暗号変換期限2905内に再暗号化を行うことによりライセンスの取り込みが可能となる。
- [0342] 図30は、本実施の形態2に係る送出装置のコンテンツDB305に記録されているコンテンツ管理テーブル3000の一例を示している。尚、このコンテンツ管理テーブル3000は、上述した実施の形態1の図8に示したコンテンツ管理テーブル800と同様の構成となるため説明を省略する。
- [0343] 図31は、本実施の形態2に係る送出装置から送信されるKc伝送用ECM3100のデータ構成の一例を示す参考図である。
- [0344] このKc伝送用ECM3100は、上述した図11に示すKc伝送用ECM1100のデータ構成である事業者ID1102、サービスタイプ1103、ワーク鍵1104、契約判定情報1105、ライセンスID1107、ライセンス有効期限1108、コンテンツ鍵Kc1109、利用可能回数1110、書き出し可能回数1111、改ざん検出1112に加えて、送出装置の

ECM生成部2801において付与され、受信装置側で再暗号化を行うことができる期限である暗号変換期限3101が付与されている点異なる。また、ECM-Kw及びECM-Kcと同様に、セクションヘッダ1101、セクションテラ(誤り検出)1113が付与されているのは図11と同様である。

[0345] 図32は、本実施の形態2に係る受信装置のシステム構成を示す参考図である。端末装置102の機能構成は上述した実施の形態1に係る図23の端末装置102と同様の構成となるが、本実施の形態2において、ICカード103には、ECM再暗号化部3201、ライセンス取り込み処理部3202、及び取り込み履歴データベース3203が備えられている。

[0346] ライセンス取り込み処理部3202は、蓄積固有鍵 K_m' で暗号化されたKc伝送用ECMの復号結果を確認すると共に、端末装置102側の蓄積部1203からICカード103のライセンスDB1212へのライセンス取り込み時においては、ライセンス取り込み処理を行う。

[0347] 取り込み履歴データベース3203は、ECM再暗号化部3201においてマーキングが付与されたライセンス、すなわち、暗号変換が行われたライセンスであり、ライセンス取り込み処理部3202においてICカード103へ取り込みが可能と判断されたライセンスのライセンスIDを、取り込み履歴DB3203として管理する。

[0348] ECM再暗号化部3201は、送出装置からのライセンス受信時に、蓄積固有鍵 K_m' によるKc伝送用ECMの暗号変換の処理を行う。即ち、ECM再暗号化部3201は、契約が行われて、且つ暗号変換期限内であるライセンスに対して蓄積暗号鍵 K_m' を用いてマーキング処理を行う。

[0349] 図33は、本実施の形態2に係る受信装置側のICカード103の取り込み履歴DB3203に記録されている取り込み履歴テーブル(IL:Import List) 3300の一例を示す参考図である。尚、本図に示す取り込み履歴テーブル3300は、実施の形態1の図15に係る取り込み履歴テーブル1500とほぼ同様であるが、図15のライセンス変換期限1502の代わりにライセンスID3301に対応したライセンスの有効期限3302が記述されている。

[0350] 図34は、本実施の形態2に係る放送局101における送出装置が、コンテンツを送

出する動作手順を示すフローチャートである。

- [0351] まず、送出装置のECM生成部2801は、図31に示すように、暗号変換期限3101を付与したKc伝送用ECM3100を生成する(ステップS3401)。
- [0352] 具体的には、ECM生成部2801は、ECM生成指示をトリガとして、コンテンツ単位の暗号鍵を有するKc伝送用ECM3100を生成するため、コンテンツ属性情報DB303およびコンテンツ鍵DB304を参照して、ライセンスID2902、利用条件2903などを読み出す。読み出した情報から、図31に示したKc伝送用ECM3100を生成する。そして、ECM生成部2801は、生成したKc伝送用ECM3100を、ECM暗号化部311に送信する。尚、S1802～S1809の処理は図18に示す送出装置の処理手順と同様であるために、その説明を省略する。
- [0353] 図35は、本実施の形態2に係る端末装置102およびICカード103におけるコンテンツ受信および暗号変換処理を示すフローチャートである。ただし、本処理において、ICカード103における暗号変換可否判定処理(ステップS3501)については、別途、図36に示すフローチャートを用いて詳細を説明する。
- [0354] まず、端末装置102における蓄積管理部1204は、蓄積部1203に蓄積するコンテンツの蓄積状況を監視し、コンテンツ蓄積が終了しているか否かを確認する(ステップS1901)。
- [0355] そして、ステップS1901において、YESである場合、すなわち、コンテンツの蓄積が未完了である場合には、ステップS1902を実行する。一方、ステップS1901において、NOである場合、すなわち、コンテンツの蓄積が完了した場合には、本コンテンツ蓄積処理を終了する。
- [0356] また、分離部1202は、Kc伝送用ECM3100を取得したか否かを判断する(ステップS1902)。
- [0357] 次に、ステップS1902において、YESである場合、すなわち、Kc伝送用ECM3100を未取得である場合には、ステップS1903を実行する。一方、ステップS1902において、NOである場合、すなわち、Kc伝送用ECM3100を取得済みである場合には、ステップS1911を実行する。
- [0358] また、分離部1202は、Kc伝送用ECM3100を分離し、ICカード103に送信する(

ステップS1903)。

- [0359] そして、ICカード103における処理においては、ライセンス取り込み処理部3202はKc伝送用ECM3100の暗号変換期限を参照して、暗号変換可否判定処理を行う(ステップS3501)。尚、この暗号変換可否判定(ステップS3501)の処理の詳細は図36のフローチャートにおいて説明する。
- [0360] 次に、ECM再暗号化部3201は、ステップS3051において暗号変換可否判定を行った結果を用いて、ライセンスの再暗号化が可能であるか否かの判定を行い(ステップS3502)、暗号変換がOKの場合には(ステップS3502でYES)、ECM再暗号化部3201は、Kc伝送用ECM3100を蓄積暗号鍵Km'で再暗号化(マーキング化)して暗号変換する処理を行う(ステップS3503)。一方、暗号変換がNOの場合には(ステップS3502でNO)、蓄積暗号鍵Km'により再暗号化が行われていない(すなわちマーキングが付与されていない)Kc伝送用ECM3100をレスポンスで端末装置102側に送信する(ステップS1910)。
- [0361] なお、ステップS3502において、ECM再暗号化部3201の再暗号化がNOである場合のように、当該コンテンツのライセンスの暗号変換が許可されていない場合には、その旨をメッセージとしてユーザに提示することも可能である。また、この場合、必ずしも、蓄積暗号鍵Km'により再暗号化が行われていない(すなわちマーキングが付与されていない)Kc伝送用ECM3100を、端末装置102側に送信しなくても良い。
- [0362] そして、端末装置102の第1のカードI/F部1207は、ICカード103からのレスポンスを受信する(ステップS1910)。具体的には、第1のカードI/F部1207は、ICカード103の第2のカードI/F部1213から、Kc伝送用ECM1100の送信に対するレスポンスを受信する。
- [0363] また、端末装置102の蓄積管理部1204は、コンテンツ、ECM-Kc、及び、ICカード103から返信された蓄積暗号鍵Km'により再暗号化が行われたKc伝送用ECM2100を蓄積部1203に蓄積する処理を行う(ステップS1911)。以上、図35を用いて、端末装置102及びICカード103におけるコンテンツ蓄積処理についての説明を行った。
- [0364] 図36は、本実施の形態2に係る端末装置102における暗号変換可否判定処理(図

35のS3501に対応)における動作手順を示すフローチャートである。

- [0365] まず、ICカード103のECM／EMM復号部1214は、カード管理情報DB1210を参照して、Kc伝送用ECM3100を復号するためのワーク鍵Kw203が存在するか否かを判定する(ステップS2101)。
- [0366] そして、ステップS2101において、YESである場合、すなわち、ワーク鍵Kw1406が存在する場合には、ステップS2102を実行する。一方、ステップS2101において、NOである場合、すなわち、ワーク鍵Kw1406が存在しない場合には、ステップS3603を実行する。
- [0367] そして、ECM／EMM復号部1214は、ワーク鍵Kw1406でKc伝送用ECM3100を復号する(ステップS2102)。
- [0368] また、ECM／EMM処理部1215は、ICカード103が、当該コンテンツを視聴するための契約を有しているか否かを判定する(ステップS2103)。具体的には、ECM／EMM処理部1215は、Kc伝送用ECM3100の契約判定情報1105と、カード管理情報DB1210に記録されている事業者別情報テーブル1400のティア契約ID1402またはPPV契約ID1403を比較して、いずれかのIDが一致するか否かの判定処理を行う。また、合わせて、カード管理情報DB1210に記録されている事業者別情報テーブル1400の有効期限1404を参照して、現在時刻が有効期限1404内であるか否かを確認する。この場合の現在時刻は、端末装置102がICカード103に対して、図32の端末装置102に図示しない現在時刻管理部で取得した現在時刻を、ステップS1910でKc伝送用ECM2100とともに送信する。
- [0369] そして、ステップS2103において、YESである場合、すなわち、いずれかのIDが一致し、かつ、現在時刻が有効期限1404内である場合には、ステップS3601を実行する。一方、ステップS2103において、NOである場合、すなわち、いずれのIDも一致しない場合、または、現在時刻が有効期限1404外である場合には、ステップS3603を実行する。
- [0370] 次に、ECM再暗号化部3201は、Kc伝送用ECM3100に記述されている暗号変換期限内か否かの判定を行い(ステップS3601)、暗号変換期限内である場合には(ステップS3601でYES)、マーキング可能とし、蓄積暗号鍵Km'を用いてKc伝送用

ECM3100を再暗号化するための暗号変換の許可を行い(ステップS3602)、一方、ライセンス取り込み処理部3202は、暗号変換期限内でない場合には(ステップS3602でNO)、Kc伝送用ECM3100の再暗号化を不許可とする(ステップS3603)。

[0371] 具体的には、ステップS3601において、ライセンス取り込み処理部3202は、Kc伝送用ECM3100の暗号変換期限3101を参照して、端末装置102からKc伝送用ECM3100と一緒に取得した現在時刻と比較することにより、当該Kc伝送用ECM3100が暗号変換期限内であるか否かを判定する。

[0372] 図37は、本実施の形態2に係る端末装置102およびICカード103におけるライセンス取り込み時における処理手順を示すフローチャートである。ただし、本処理において、ICカード103におけるライセンス取り込み可否判定処理(ステップS3702に対応)については、別途、図38に示すフローチャートを用いて説明する。

[0373] なお、このライセンス取り込み時における処理は、当該ライセンスに対応するコンテンツの視聴前に行われれば良いが、ユーザがコンテンツを視聴する際に行っても良い。

[0374] 最初に、端末装置102の蓄積部1203に蓄積されたKc伝送用ECM3100をICカードに送信する処理を行う(ステップS3701)。

[0375] 次に、ICカード103は、受信したKc伝送用ECM3100のライセンス取り込み可否判定処理を行う(ステップS3702)。

[0376] 具体的には、ICカード103の第2のカードI/F部1213は、端末装置102の第1のカードI/F部1207が送信した、Kc伝送用ECM3100を受信し、ライセンス取り込み処理部3202は、Kc伝送用ECM3100がマーキングされているか、即ち、蓄積暗号鍵Km¹により再暗号化されているかを確認することにより、ライセンス取り込み処理を行ってもよいか否かの判定処理を実行する。なお、本ライセンス取り込み可否判定処理の詳細については、図38を用いて詳細を説明する。

[0377] ICカード103のライセンス取り込み処理部3202は、ライセンス取り込み可否判定処理の結果、ライセンスの取り込みが許可されているか否かを確認する(ステップS3703)。

[0378] ステップS3703において、YESである場合、すなわち、ライセンス取り込みが許可

されている場合には、ステップS3704を実行する。一方、ステップS3703において、NOである場合、すなわち、ライセンス取り込みが許可されていない場合には、ライセンスの取り込みは行われず、ステップS3707を実行する。

[0379] そして、ステップS3703においてYESである場合、ライセンス取り込み処理部3202は、Kc伝送用ECM3100をライセンス変換し、図16に示すような蓄積視聴用のライセンス1600を生成する(ステップS3704)。具体的には、ライセンス取り込み処理部3202は、Kc伝送用ECM3100に含まれるライセンスID1107、ライセンス有効期限1108などを取得して、ライセンス1600を生成する。

[0380] 次に、ライセンス取り込み処理部3202は、当該ライセンスの変換履歴を取り込み履歴DB3203に記録する(ステップS3705)。具体的には、ライセンス取り込み処理部3202は、取り込み履歴DB3203に蓄積されているTL1500のライセンスID1501と有効期限に、Kc伝送用ECM3100のライセンスID1107と有効期限1108を追加する。

[0381] そして、ライセンス処理部1217は、取り込んだライセンスをライセンスDB1212に蓄積する処理を行う(ステップS3706)。

[0382] 次に、第2のカードI/F部1213は、端末装置102に対して、Kc伝送用ECM3100によるライセンス変換要求に対するレスポンスを送信する(ステップS3707)。具体的には、第2のカードI/F部1213は、当該コンテンツのライセンス取り込みが許可されており、ライセンス取り込みが完了したか、あるいは、当該コンテンツのライセンス取り込みが許可されていない、または、ライセンス取り込みに失敗した、などのレスポンスメッセージを生成して、端末装置102に送信する。

[0383] そして、第1のカードI/F部1213は、ICカード102からKc伝送用ECM3100によるライセンス変換要求に対するレスポンスを送信する(ステップS3708)。

[0384] なお、ステップS3703において、NOである場合のように、当該コンテンツのライセンス取り込みが許可されていない場合には、その旨のメッセージをユーザに提示するようにしても良い。

[0385] また、取り込んだライセンスをICカード103のライセンスDB1212に蓄積せず、端末装置102に蓄積する場合には、ステップS3706において、取り込んだライセンスのラ

イセンスID、ハッシュ値などをICカード103に蓄積して、ステップS3707において端末装置102に取り込んだライセンスをレスポンスとして送信すれば良い。

- [0386] 図38は、本実施の形態2に係る受信装置において、図37で示したライセンス取り込み可否判定(ステップS3702に対応)の具体的な動作手順を示すフローチャートである。
- [0387] まず、ICカードのECM/EMM復号部1214は、カード管理情報DB1210を参照して、Kc伝送用ECM3100を復号するための蓄積暗号鍵Km' 203が存在するか否かを判定する(ステップS3801)。
- [0388] 具体的には、ECM/EMM復号部1214は、カード管理情報DB1210を参照してカードIDに対応する蓄積暗号鍵Km'を読み出す。このとき、Kc伝送用ECM3100のカードIDと蓄積暗号鍵Km'が一致しない場合などは、蓄積暗号鍵Km'が存在しないものとして処理する(ステップS3801でNO)。
- [0389] そして、ステップS3801において、YESである場合、すなわち、蓄積暗号鍵Km'が存在する場合には、ステップS3802を実行する。一方、ステップS3801において、NOである場合、すなわち、蓄積暗号鍵Km'が存在しない場合には、ライセンスの取り込みを不許可とするステップS2111を実行する。
- [0390] 次に、ECM/EMM復号部1214は、蓄積暗号鍵Km'でKc伝送用ECM1100を復号可能か否かの判定を行う(ステップS3802)。
- [0391] 具体的には、ECM/EMM復号部1214は、ステップS3801で取得した蓄積暗号鍵Km'で、AESによりKc伝送用ECM3100の暗号化部を復号し、Kc伝送用ECM3100の改ざん検出1110により、Kc伝送用ECM3100が改ざんされていないかを確認して蓄積暗号鍵Km'で復号できるかの判定を行う。また、Kc伝送用ECM3100が改ざんされていることが検出された場合には、ライセンス取り込みは許可できないので、ステップS2111を実行して、本処理を終了する。
- [0392] そして、蓄積暗号鍵Km'でKc伝送用ECM1100を復号可能な場合には(ステップS3802でYES)、ライセンス取り込み処理部3202は、Kc伝送用ECM3100がライセンスの有効期限内であるかどうかを判定する(ステップS3803)。具体的には、ライセンス取り込み処理部3202は、Kc伝送用ECM3100のライセンスの有効期限110

8を参照して、端末装置102からKc伝送用ECM3100と一緒に取得した現在時刻と比較することにより、当該Kc伝送用ECM3100が有効期限内であるか否かを判定する。

[0393] そして、ステップS3803において、YESである場合、すなわち、有効期限1108が現在時刻よりも新である場合には、有効期限内であると判定し、ステップS2105を実行する。一方、ステップS3803において、NOである場合、すなわち、有効期限1108が現在時刻よりも旧である場合には、有効期限外であると判定し、ステップS2111を実行する。

[0394] なお、ステップS3803の有効期限の判定処理については、もはや有効期限が経過した、不要なライセンスを蓄積しないようにするために行うものであるので、本処理は省略することも可能である。

[0395] ライセンス取り込み処理部3202は、取り込み履歴DB3203を参照して、該当ライセンスIDの変換履歴を検索する(ステップS2105)。具体的には、ライセンス取り込み処理部3202は、取り込み履歴DB3203のTL1500を参照し、Kc伝送用ECM3100のライセンスID1107と一致するライセンスID1501のレコードを検索する。

[0396] そして、ライセンス取り込み処理部3202は、該当ライセンスIDの変換履歴が存在するか否かを判定する(ステップS2106)。具体的には、ライセンス取り込み処理部3202は、ステップS2105の検索結果を参照し、取り込み履歴DB3203にKc伝送用ECM3100のライセンスID1107とTL1500のライセンスID1501が一致するレコードが存在するか否かを確認する。

[0397] ステップS2106において、YESである場合、すなわち、該当ライセンスIDの取り込み履歴が存在しない場合には、ステップS2107を実行する。一方、ステップS2106において、NOである場合、すなわち、該当ライセンスIDの取り込み履歴が存在する場合には、ステップS2111を実行する。

[0398] ライセンス取り込み処理部3202は、TL1500に空きレコードまたは有効期限を超過したレコードが存在するか否かを検索する(ステップS2107)。

[0399] 具体的には、ライセンス取り込み処理部3202は、新たにライセンス変換を行うライセンスIDを追記するレコードを発見するため、TL1500を参照して、空きレコードを

検索する。空きレコードが存在しない場合は、TL1500の、ライセンス変換期限1502と、端末装置102からKc伝送用ECM3100と一緒に取得した現在時刻を比較し、ライセンス変換期限1502が現在時刻より新であるレコードを検索する。

[0400] ライセンス取り込み処理部3202は、変換履歴DB1211に空きレコードもしくはライセンス変換期限を超過しているレコードが存在するか否かを判定する(ステップS2108)。具体的には、ライセンス取り込み処理部3202は、ステップS2107の検索結果を参照し、TL1500に空きレコードをもしくはライセンス変換期限1502を超過しているレコードが存在するか否かを判定する。

[0401] ステップS2108において、YESである場合、すなわち、空きレコードまたはライセンス変換期限1502を超過しているレコードが存在する場合には、ステップS2109を実行する。一方、ステップS2108において、NOである場合、すなわち、空きレコードまたはライセンス変換期限1502を超過しているレコードが存在しない場合には、これ以上ライセンス変換を実行することはできないため、ステップS2111を実行する。

[0402] そして、ライセンス取り込み処理部3202は、ステップS2108で判定した結果に基づき、空きレコードがない場合には、ライセンス変換期限1502を超過したレコードを削除し、新たなライセンスID1501の追加をできるようにする(ステップS2109)。

[0403] ライセンス取り込み処理部3202は、当該Kc伝送用ECM3100のライセンス変換を許可と判定し、本ライセンス変換可否判定処理を終了する(ステップS2110)。また、ライセンス取り込み処理部3202は、当該Kc伝送用ECM3100のライセンスを変換は不許可と判定し、本ライセンス変換可否判定処理を終了する(ステップS2111)。

[0404] 尚、本実施の形態2において図面を用いて説明はしないが、ライセンスをICカード103のライセンスDB1212に取り込んだ後のコンテンツ再生時の処理手順は上述した図22に示す処理と同様となるため説明を省略する。

[0405] 以上の説明のように、本実施の形態2に係るデジタル権利管理システムにおいては、送出装置側においてはKc伝送用ECM3100に暗号変換期限を付与する。そして、受信装置側では、受信したKc伝送用ECM3100が暗号変換期限内か否かを判定して、暗号変換期限内である場合にはECM再暗号化部3201において蓄積暗号鍵 K_m' を用いて取得したライセンスの再暗号化を行うと共に、再暗号化後のライセンス

をICカード103側から端末装置102側に返信して蓄積部1203に格納する。

- [0406] このことにより、コンテンツの視聴するため端末装置102の蓄積部1203に蓄積されているKc伝送用ECM3100をICカード103に取り込む場合、ICカード103のライセンス取り込み処理部3202は、端末装置102の蓄積部1203から取得したKc伝送用ECM3100が、蓄積暗号鍵 K_m' を用いて復号可能か否かを判定して、復号可能であるKc伝送用ECM3100のみ取り込みを行う。従って、ユーザが実際に視聴するコンテンツに関連するライセンスのみをICカード103に取り込むことができ、ライセンスに関する情報が端末装置102側で記録されるため、メモリ容量に限定のあるICカード103の容量を圧迫してしまうという問題を回避することが可能となる。
- [0407] また、Kc伝送用ECM3100に付与された暗号変換期限に基づき、暗号変換期限を制御することにより、結果としてライセンスの取り込み可能期間を制御することが可能であるため、契約されていない時期に蓄積したライセンスの不正使用を防止することが可能となる。
- [0408] さらに、本発明においては、取り込み履歴DB3203においてライセンスID3301及び有効期限3302が記録された取り込み履歴テーブル3300を管理しているために、有効期限3302を越えたライセンスの使用を適切に防止することが可能となる。
- [0409] 尚、本実施の形態2の説明においては、ICカード103のECM再暗号化部3201は、蓄積暗号鍵 K_m' を用いてKc伝送用ECM3100の再暗号化を行ったが、本発明はこれに限定されるものではなく、例えば、受信済みフラグ付与、端末／カードID付与、署名付与等、他のマーキング方法を用いてKc伝送用ECM3100の再暗号化を行うことも可能である。さらに、Kc伝送用ECM3100の再暗号を行う暗号鍵は、端末装置102やICカード103に固有の蓄積暗号鍵 K_m' 以外に、複数の端末装置102で共通の暗号鍵などを用いるようにしても良い。
- [0410] また、本実施の形態2の説明においては、送信側でKc伝送用ECM3100に暗号変換期限を付与するようにしたが、送信側で暗号変換期限を付与されない場合は、端末装置102側におけるKc伝送用ECM3100の暗号変換の際に、一定の条件に基づいて、暗号変換可否を決定するようにしても良い。例えば、Kc伝送用ECM3100(ライセンス)の有効期限から一定日数前を暗号変換期限とする場合や、端末装置

102側からKc伝送用ECM3100と共に受信した現在時刻に基づいて暗号変換期限を決定する場合などが考えられる。

[0411] (変形例)

次に、受信装置側でのライセンス取り込みの変形例について図39から図42を用いて説明を行う。尚、本変形例においては、パッケージIDと、ライセンスID(取得済みライセンスID)と、有効期限とによりライセンスの取り込みを管理することを特徴としている。

[0412] 図39は、本変形例に係るICカード103が管理するPPC(Pay Per Content、都度購入コンテンツ)用の取り込み履歴テーブル(IL:Import List)3900の図である。このPPC用のIL3900の各レコードは、PPCのコンテンツ(パッケージ)を購入した際に生成される。

[0413] 上述した取り込み履歴テーブルとの差異は、パッケージID3901とパッケージ内ライセンスID3903が記載されている点である。ここでパッケージID3901とは、購入したパッケージを識別するための情報であり、例えば「PKG-ID-1」と記述され、コンテンツの購入単位を示している。そして、パッケージの中には複数コンテンツ(例えばドラマの10話パック)が含まれる場合があり、これらはパッケージID3901に対応するパッケージ内ライセンスID3903として管理される。尚、同一ライセンスが異なるパッケージに含まれる場合も考えられ、例えばスポーツパッケージとJリーグパッケージがあり、Jリーグに関するコンテンツが両方に含まれる場合などもありうる。

[0414] 有効期限3902は、パッケージID3901に対応する有効期限であり、パッケージ内のライセンスの有効期限のうち、最も長い(有効期限が遅いもの)ものが記載される。

[0415] パッケージ内ライセンスID3903とは、パッケージに含まれるライセンスのIDの一覧であり、例えば「LICENSE-ID-1, LICENSE-ID-2, , ,」と記述され、これによりユーザに対してパッケージ内のライセンス取得状況の提示が可能となる。尚、このパッケージ内ライセンスID3902は、取り込み履歴の管理上は、必ずしも必要な情報ではなく、取得済みライセンスID3904と合わせて、ユーザに対してパッケージに含まれるライセンスと既に取得したライセンスとの関係を提示したりする場合などに用いることを想定している。

- [0416] 取得済みライセンスID3904は、パッケージ内ライセンスID3903に対して、取り込み済みのライセンスIDを示し、例えば「LICENSE-ID-1, LICENSE-ID-2」と記述される。
- [0417] 尚、このような取り込み履歴テーブル3900で管理する情報については、パッケージID3901やパッケージ内ライセンスID3903の割当方法(グローバルでユニークになるようにIDを振るか、サービスプロバイダ毎にユニークなIDを振るか)によって、管理方法が変わる場合がある。
- [0418] 図40は、本変形例に係る送出装置からの受信装置に配信されるKc伝送用ECM4000の一例を示す参考図である。本変形例に係るKc伝送用ECM4000には、PPC用の取り込み履歴テーブルで追加となり、ライセンスの取り込みの際、取り込み履歴DB3203の取り込み履歴テーブル3900に記録されるパッケージID3901に対応するパッケージID4002、及び図39に示すパッケージ内ライセンスID3903に対応するパッケージ内ライセンスID4003、及び実施の形態2と同様に暗号変換期限4001が記述されている。尚、パッケージ内ライセンスID4003は、パッケージ内に含まれるライセンスIDのリストであり、同一パッケージ内のKc伝送用ECM4000では同じ値が送信される。
- [0419] 図41は、本変形例に係る受信装置でのPPCのライセンス取り込みにおける処理手順を示すフローチャートである。尚、本図に示すライセンス取り込み可否判定処理(ステップS4102に対応)の処理については、図42において詳細に説明する。
- [0420] 最初に、端末装置102の蓄積部1203に蓄積された、Kc伝送用ECM4000をICカードに送信する処理を行う(ステップS4101)。
- [0421] 次に、ICカード103は、受信したKc伝送用ECM4000のライセンス取り込み可否判定処理を行う(ステップS4102)。
- [0422] そして、ICカード103のライセンス取り込み処理部3202は、ライセンス取り込み可否判定処理の結果、ライセンスの取り込みが許可されているか否かを確認する(ステップS4103)。
- [0423] ステップS4103において、YESである場合、すなわち、ライセンス取り込みが許可されている場合には、ステップS4104を実行する。一方、ステップS4103において、

NOである場合、すなわち、ライセンス取り込みが許可されていない場合には、ライセンスの取り込みは行われず、ステップS4107を実行する。

- [0424] そして、ステップS4103においてYESである場合、ライセンス取り込み処理部3202は、Kc伝送用ECM4000をライセンス変換し、図16に示すような蓄積視聴用のライセンス1600を生成する(ステップS4104)。
- [0425] 次に、ライセンス取り込み処理部3202は、当該ライセンスの変換履歴を取り込み履歴DB3203に記録する(ステップS4105)。具体的には、ライセンス取り込み処理部3202は、パッケージ内での最初のライセンスを取得する場合においては、取り込み履歴テーブル3900の、パッケージID3901、有効期限3902、パッケージ内ライセンスID3903、取得済みライセンスID3904を取り込み履歴DB3203に記録する。また、パッケージ内で2回目以降のライセンス取得の場合、取り込み履歴テーブル3900の取得済みライセンスID3904のみを取り込み履歴DB3203に記録する処理を行う。これは、他の項目は既に記録済みであるためである。
- [0426] そして、ライセンス処理部1217は、取り込んだライセンスをライセンスDB1212に蓄積する処理を行う(ステップS4106)。
- [0427] 次に、第2のカードI/F部1213は、端末装置102に対して、Kc伝送用ECM4000によるライセンス変換要求に対するレスポンスを送信する(ステップS4107)。
- [0428] 図42は、図41で示したライセンス取り込み可否判定(ステップS4102に対応)の具体的な動作手順を示すフローチャートである。
- [0429] まず、ICカード103のECM/EMM復号部1214は、カード管理情報DB1210を参照して、Kc伝送用ECM4000を復号するための蓄積暗号鍵Km'が存在するかどうかを判定する(ステップS4201)。
- [0430] そして、ステップS4201において、YESである場合、すなわち、蓄積暗号鍵Km'が存在する場合には、ステップS4202を実行する。一方、ステップS4201において、NOである場合、すなわち、蓄積暗号鍵Km'が存在しない場合には、ライセンスの取り込みを不許可とするステップS2111を実行する。
- [0431] 次に、ECM/EMM復号部1214は、蓄積暗号鍵Km'でKc伝送用ECM1100の復号を行う(ステップS4202)。

- [0432] そして、蓄積暗号鍵 K_m でKc伝送用ECM4000を復号すると、ライセンス取り込み処理部3202は、Kc伝送用ECM4000がライセンスの有効期限内であるかどうかを判定する(ステップS4203)。
- [0433] そして、ステップS4203において、YESである場合、すなわち、有効期限1108が現在時刻よりも新である場合には、有効期限内であると判定し、ステップS4204を実行する。一方、ステップS4203において、NOである場合、すなわち、有効期限1108が現在時刻よりも旧である場合には、有効期限外であると判定し、ステップS2111を実行する。
- [0434] ライセンス取り込み処理部3202は、取り込み履歴DB3203を参照して、該当ライセンスIDの変換履歴を検索する(ステップS4204)。具体的には、ライセンス取り込み処理部3202は、取り込み履歴DB3203のTL1500を参照し、Kc伝送用ECM4000のパッケージID4002とライセンスID4003との組に基づいて、レコードの一致／不一致を検索する。
- [0435] そして、ライセンス取り込み処理部3202は、該当パッケージIDとライセンスIDの変換履歴が存在するか否かを判定する(ステップS2106)。具体的には、ライセンス取り込み処理部3202は、ステップS2105の検索結果を参照し、取り込み履歴DB3203にKc伝送用ECM4000のパッケージID4002とパッケージ内ライセンスID4003との組と、取り込み履歴テーブル3900のパッケージID3901とパッケージ内ライセンスID3903との組が一致するレコードが存在するか否かを確認する。
- [0436] ステップS2106において、YESである場合、すなわち、該当パッケージIDとライセンスIDの変換履歴が存在しない場合には、ステップS2107を実行する。一方、ステップS2106において、NOである場合、すなわち、該当パッケージIDとライセンスIDの変換履歴が存在する場合には、ステップS2111を実行する。尚、S2107以下の処理は上述の図38と同様であるために、その説明を省略する。
- [0437] 以上のように、本変形例においては、Kc伝送用ECM4000に含まれるパッケージID4002、パッケージ内ライセンスID4003及び有効期限1108を用いて、パッケージID4002とパッケージ内ライセンスID4003とが重複するライセンスの取得を抑制して、受信装置のICカード103におけるライセンスの取り込み管理を行う。従って、パッケ

ージに対してパッケージID3901を割り当てて、パッケージ内に含まれる複数のコンテンツに割り当てられるパッケージ内ライセンスID3903を異なるパッケージにおいても統一的に管理することができるために、小メモリ容量のICカード103の効率的な利用を行いライセンスの不正使用を防止すると共に、例えばドラマの3ヶ月間で12回放送されるシリーズ番組やコンテンツを一度に多数購入する場合など、実際のユーザの利用により適したライセンスデータの管理を行うことが可能となる。

産業上の利用可能性

- [0438] 本発明にかかるデジタル権利管理システムは、端末装置で取得したライセンスIDと有効期限とを合わせてリストで管理し、少なくともライセンスの有効期限までレコードと保持することにより、不正なライセンス取得の防止と、管理するデータサイズの増大の防止とを両立できるという効果を有し、デジタル放送、デジタルCATV、インターネットなどによるコンテンツ配信サービスにおけるデジタル権利管理システムなどとして有用である。またパッケージメディアなどの可搬メディアなどによるコンテンツ配信サービスにおけるデジタル権利管理システムにも応用できる。

請求の範囲

- [1] コンテンツの利用許諾を与えるためのライセンスを配信する送出装置から、前記ライセンスを取得し、当該ライセンスに基づき前記コンテンツを利用する受信装置であつて、
- 前記ライセンスには、少なくとも前記ライセンスを前記受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限及びライセンスIDが付与され、
- 前記受信装置は、
- 前記送出装置から送出される前記ライセンスを取り込むライセンス取り込み手段と、
- 少なくとも前記ライセンス取り込み期限まで、前記ライセンスIDと前記ライセンス取り込み期限とを含むライセンス取り込み履歴を記録する履歴記録手段と、
- 前記ライセンス取り込み手段において取り込んだライセンスのライセンスIDと同一のライセンスIDが前記ライセンス取り込み履歴に存在する場合に、前記ライセンス取り込み手段における当該ライセンスの取り込みを抑制するライセンス取り込み抑制手段とを備える
- ことを特徴とする受信装置。
- [2] 前記受信装置は、さらに、
- 前記ライセンス取り込み手段で取り込む前の暗号化ライセンスを一旦復号して、復号済みライセンスを生成するライセンス復号手段と、
- 前記暗号化ライセンスの暗号化に用いた暗号鍵とは異なる暗号鍵を用いて、前記復号済みライセンスを再暗号化して再暗号化ライセンスを生成する再暗号化手段と、
- 少なくとも前記再暗号化ライセンスを蓄積する蓄積手段とを備える
- ことを特徴とする請求項1記載の受信装置。
- [3] 前記ライセンスには、さらに、前記再暗号化手段における再暗号化が可能な期限である暗号変換期限が付加され、
- 前記再暗号化手段は、前記暗号変換期限内のライセンスに対して再暗号化を行って前記再暗号化ライセンスを生成し、前記再暗号化ライセンスを前記蓄積手段に蓄積する
- ことを特徴とする請求項2記載の受信装置。

- [4] 前記受信装置は、前記コンテンツの再生を行う端末装置と、当該端末装置と連携されるセキュリティモジュールとから構成され、
 前記蓄積手段は、前記端末装置に備えられ、
 前記ライセンス取り込み手段、前記履歴記録手段、前記ライセンス取り込み抑制手段及び前記再暗号化手段の少なくとも1つは、前記セキュリティモジュールに備えられ、
 前記再暗号化手段において用いられる暗号鍵は、前記セキュリティモジュールまたは前記端末装置に固有の蓄積暗号鍵であることを特徴とする請求項3記載の受信装置。
- [5] 前記受信装置は、さらに、
 前記ライセンスが、前記再暗号化されているか否かを判定し、前記再暗号化されている場合において前記再暗号化されたライセンスを復号する再暗号化ライセンス復号手段を備える
 ことを特徴とする請求項3記載の受信装置。
- [6] 前記受信装置は、さらに、
 前記ライセンス取り込み手段で取得する前記ライセンスにかかわる契約がなされているかを判定する契約判定手段を備え、
 前記ライセンス取り込み手段は、前記契約判定手段において契約されていると判定された場合、前記ライセンス取り込み期限内か否かを判定し、ライセンス取り込み期限内である場合には、ライセンス取り込みの許可を行う
 ことを特徴とする請求項1記載の受信装置。
- [7] 前記受信装置は、前記コンテンツの再生を行う端末装置と、当該端末装置と連携されるセキュリティモジュールとから構成され、
 前記契約判定手段は、前記セキュリティモジュールに備えられる
 ことを特徴とする請求項6記載の受信装置。
- [8] 前記履歴記録手段には、さらに、前記ライセンス取り込み手段において前記ライセンスを取り込んだ場合には、取り込まれた前記ライセンスのライセンスIDと、前記ライセンスの有効期限とが含まれたライセンス取り込み履歴が記録される

ことを特徴とする請求項1記載の受信装置。

- [9] 前記受信装置は、さらに、
前記ライセンスに前記ライセンス取り込み期限が設定されていない場合には、前記ライセンス取り込み履歴の前記ライセンス取り込み期限を生成するライセンス取り込み期限生成手段を備え、
前記履歴記録手段は、前記ライセンスIDと生成された当該ライセンス取り込み期限を含むライセンス取得履歴を記録する
ことを特徴とする請求項1記載の受信装置。
- [10] 前記ライセンスは、さらに、ライセンス取り込み条件が付与され、
前記ライセンス取り込み抑制手段は、前記ライセンス取り込み条件に基づき、前記ライセンスの取り込みを制御する
ことを特徴とする請求項1記載の受信装置。
- [11] 前記受信装置は、さらに、
前記ライセンス取り込み抑制手段において前記ライセンスの取り込みを行わない場合に、少なくとも、前記ライセンスの取り込みができない旨、あるいは、前記ライセンスの取り込みができない理由を提示するメッセージ提示手段を備える
ことを特徴とする請求項1記載の受信装置。
- [12] 前記ライセンス取り込み期限は、前記ライセンスの有効期限である、又は、前記ライセンスの有効期限とは別に設定される期限である
ことを特徴とする請求項1記載の受信装置。
- [13] 前記ライセンスには、さらに、前記コンテンツの購入単位であるパッケージの識別番号であるパッケージIDと、前記パッケージ内に含まれるライセンスの識別番号であるパッケージ内ライセンスIDと、当該ライセンスの有効期限とが付与され、
前記履歴管理手段は、前記パッケージ内での最初のライセンスの取得においては、前記パッケージIDと、前記パッケージ内ライセンスIDと、前記有効期限と、既に取得した取得済みライセンスIDとを含むライセンス取得履歴を記録し、
前記履歴管理手段は、前記パッケージ内での2回目以降のライセンスの取得においては、前記ライセンス取得履歴の取得済みライセンスIDのみを更新して記録し、

前記ライセンス取り込み抑制手段は、前記パッケージIDと前記パッケージ内ライセンスIDとの組と同一の組が前記ライセンス取得履歴に存在する場合に、前記取得手段における前記ライセンスの取得を抑制する

ことを特徴とする請求項1記載の受信装置。

- [14] コンテンツの利用許諾を与えるためのライセンスに基づきコンテンツを利用する受信装置に対して前記ライセンスを送出する送出装置であって、

前記ライセンスを生成するライセンス生成手段と、

前記ライセンスに、識別番号であるライセンスIDを付与するライセンスID付与手段と、

前記ライセンスに、前記受信装置において、少なくとも当該ライセンスを当該受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限を付与するライセンス取り込み期限付与手段と、

少なくとも前記ライセンスID、前記ライセンス取り込み期限が付与された前記ライセンスを、前記受信装置に送出する送出手段とを備える

ことを特徴とする送出装置。

- [15] 前記受信装置は、前記ライセンスの暗号化に用いた暗号鍵とは異なる暗号鍵を用いて、前記復号済みライセンスを再暗号化して再暗号化ライセンスを生成する再暗号化手段を備え、

前記送出装置は、さらに、

前記ライセンスに、前記再暗号化手段における再暗号化が可能な期限である暗号変換期限を付加する暗号変換期限付与手段を備え、

前記送出手段は、少なくとも前記ライセンスID、前記暗号変換期限が付与されたライセンスを、前記受信装置に送出する

ことを特徴とする請求項14記載の送出装置。

- [16] 前記送出装置は、さらに、

前記ライセンスに前記ライセンス取り込み期限を付与するか否かを決定するライセンス取り込み期限付与決定手段を備える

ことを特徴とする請求項14記載の送出装置。

- [17] 前記送出装置は、さらに、
前記ライセンスにライセンス取得条件を付与するライセンス取得条件付与手段を備える
ことを特徴とする請求項14記載の送出装置。
- [18] 前記送出装置は、さらに、
前記ライセンスを暗号化して暗号化ライセンスを生成するライセンス暗号化手段を備える
ことを特徴とする請求項14記載の送出装置。
- [19] 前記ライセンス取り込み期限は、前記ライセンスの有効期限である、又は、前記ライセンスの有効期限とは別に設定される期限である
ことを特徴とする請求項14記載の送出装置。
- [20] ライセンスに基づきコンテンツを利用する端末装置と連携して動作するセキュリティモジュールであって、
前記ライセンスには、少なくとも前記ライセンスを前記受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限及びライセンスIDが付与され、
前記セキュリティモジュールは、
前記送出装置から送出される前記ライセンスを取り込むライセンス取り込み手段と、
少なくとも前記ライセンス取り込み期限まで、前記ライセンスIDと前記ライセンス取り込み期限とを含むライセンス取り込み履歴を記録する履歴記録手段と、
前記ライセンス取り込み手段において取り込んだライセンスのライセンスIDと同一のライセンスIDが前記ライセンス取り込み履歴に存在する場合に、前記ライセンス取り込み手段における当該ライセンスの取り込みを抑制するライセンス取り込み抑制手段とを備える
ことを特徴とするセキュリティモジュール。
- [21] 前記セキュリティモジュールは、さらに、
前記ライセンス取り込み手段で取り込む前の暗号化ライセンスを一旦復号して、復号済みライセンスを生成するライセンス復号手段と、
前記暗号化ライセンスの暗号化に用いた暗号鍵とは異なる暗号鍵を用いて、前記

復号済みライセンスを再暗号化して再暗号化ライセンスを生成する再暗号化手段とを備える

ことを特徴とする請求項20記載のセキュリティモジュール。

- [22] 前記端末装置は、少なくとも前記再暗号化ライセンスを蓄積する蓄積手段を備え、前記ライセンスには、さらに、前記再暗号化手段における再暗号化が可能な期限である暗号変換期限が付加され、

前記再暗号化手段は、前記暗号変換期限内のライセンスに対して再暗号化を行って前記再暗号化ライセンスを生成し、前記再暗号化ライセンスを前記蓄積手段に蓄積する

ことを特徴とする請求項20記載のセキュリティモジュール。

- [23] 前記セキュリティモジュールは、さらに、前記ライセンス取り込み手段で取得する前記ライセンスにかかわる契約がなされているかを判定する契約判定手段を備え、

前記ライセンス取り込み手段は、前記契約判定手段において契約されていると判定された場合、前記ライセンス取り込み期限内か否かを判定し、ライセンス取り込み期限内である場合には、ライセンス取り込みの許可を行う

ことを特徴とする請求項20記載のセキュリティモジュール。

- [24] 前記セキュリティモジュールは、さらに、前記ライセンスが、前記再暗号化されているか否かを判定し、前記再暗号化されている場合において前記再暗号化されたライセンスを復号する再暗号化ライセンス復号手段を備える

ことを特徴とする請求項21記載のセキュリティモジュール。

- [25] ユーザに対して、コンテンツの利用許諾を与えるためのライセンスを配信する送出装置と、前記ライセンスを取得し前記ライセンスに基づきコンテンツをセキュアに利用する受信装置と、から構成されるデジタル権利管理システムであって、

前記送出装置は、

前記ライセンスを生成するライセンス生成手段と、

前記ライセンスに、識別番号であるライセンスIDを付与するライセンスID付与手段

と、

前記ライセンスに、前記受信装置において、少なくとも当該ライセンスを当該受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限を付与するライセンス取り込み期限付与手段と、

少なくとも前記ライセンスID、前記ライセンス取り込み期限が付与された前記ライセンスを、前記受信装置に送出する送出手段とを備え、

前記受信装置は、

前記送出装置から送出される前記ライセンスを取り込むライセンス取り込み手段と、

少なくとも前記ライセンス取り込み期限まで、前記ライセンスIDと前記ライセンス取り込み期限とを含むライセンス取り込み履歴を記録する履歴記録手段と、

前記ライセンス取り込み手段において取り込んだライセンスのライセンスIDと同一のライセンスIDが前記ライセンス取り込み履歴に存在する場合に、前記ライセンス取り込み手段における当該ライセンスの取り込みを抑制するライセンス取り込み抑制手段とを備える

ことを特徴とするデジタル権利管理システム。

[26] 前記送出装置は、さらに、

前記ライセンスに、前記再暗号化手段における再暗号化が可能な期限である暗号変換期限を付加する暗号変換期限付与手段を備え、

前記送出手段は、少なくとも前記ライセンスID、前記暗号変換期限が付与されたライセンスを、前記受信装置に送出し、

前記受信装置は、さらに、

前記ライセンス取り込み手段で取り込む前の暗号化ライセンスを一旦復号して、復号済みライセンスを生成するライセンス復号手段と、

前記暗号化ライセンスの暗号化に用いた暗号鍵とは異なる暗号鍵を用いて、前記復号済みライセンスを再暗号化して再暗号化ライセンスを生成する再暗号化手段と、
少なくとも前記再暗号化ライセンスを蓄積する蓄積手段とを備える

ことを特徴とする請求項25記載のデジタル権利管理システム。

[27] コンテンツの利用許諾を与えるためのライセンスを配信する送出装置から、前記ライ

センスを取得し、当該ライセンスに基づき前記コンテンツを利用する受信装置に用いる受信方法であって、

前記ライセンスには、少なくとも前記ライセンスを前記受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限及びライセンスIDが付与され、

前記受信方法は、

前記送出装置から送出される前記ライセンスを取り込むライセンス取り込みステップと、

少なくとも前記ライセンス取り込み期限まで、前記ライセンスIDと前記ライセンス取り込み期限とを含むライセンス取り込み履歴を記録する履歴記録ステップと、

前記ライセンス取り込みステップにおいて取り込んだライセンスのライセンスIDと同一のライセンスIDが前記ライセンス取り込み履歴に存在する場合に、前記ライセンス取り込みステップにおける当該ライセンスの取り込みを抑制するライセンス取り込み抑制ステップとを含む

ことを特徴とする受信方法。

- [28] コンテンツの利用許諾を与えるためのライセンスに基づきコンテンツを利用する受信装置に対して前記ライセンスを送出する送出装置に用いる送信方法であって、
- 前記ライセンスを生成するライセンス生成ステップと、
- 前記ライセンスに、識別番号であるライセンスIDを付与するライセンスID付与ステップと、
- 前記ライセンスに、前記受信装置において、少なくとも当該ライセンスを当該受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限を付与するライセンス取り込み期限付与ステップと、
- 少なくとも前記ライセンスID、前記ライセンス取り込み期限が付与された前記ライセンスを、前記受信装置に送出する送出ステップとを含む
- ことを特徴とする送信方法。

- [29] ライセンスに基づきコンテンツを利用する端末装置と連携して動作するセキュリティモジュールに用いるライセンス取得方法であって、
- 前記ライセンスには、少なくとも前記ライセンスを前記受信装置に取り込み、利用可

能な状態とする期限であるライセンス取り込み期限及びライセンスIDが付与され、

前記ライセンス取得方法は、

前記送出装置から送出される前記ライセンスを取り込むライセンス取り込みステップと、

少なくとも前記ライセンス取り込み期限まで、前記ライセンスIDと前記ライセンス取り込み期限とを含むライセンス取り込み履歴を記録する履歴記録ステップと、

前記ライセンス取り込みステップにおいて取り込んだライセンスのライセンスIDと同一のライセンスIDが前記ライセンス取り込み履歴に存在する場合に、前記ライセンス取り込みステップにおける当該ライセンスの取り込みを抑制するライセンス取り込み抑制ステップとを含む

ことを特徴とするライセンス取得方法。

- [30] コンテンツの利用許諾を与えるためのライセンスを配信する送出装置から、前記ライセンスを取得し、当該ライセンスに基づき前記コンテンツを利用する受信装置に用いるプログラムであって、

前記ライセンスには、少なくとも前記ライセンスを前記受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限及びライセンスIDが付与され、

前記プログラムは、

前記送出装置から送出される前記ライセンスを取り込むライセンス取り込みステップと、

少なくとも前記ライセンス取り込み期限まで、前記ライセンスIDと前記ライセンス取り込み期限とを含むライセンス取り込み履歴を記録する履歴記録ステップと、

前記ライセンス取り込みステップにおいて取り込んだライセンスのライセンスIDと同一のライセンスIDが前記ライセンス取り込み履歴に存在する場合に、前記ライセンス取り込みステップにおける当該ライセンスの取り込みを抑制するライセンス取り込み抑制ステップと

をコンピュータに実行させることを特徴とするプログラム。

- [31] コンテンツの利用許諾を与えるためのライセンスに基づきコンテンツを利用する受信装置に対して前記ライセンスを送出する送出装置に用いるプログラムであって、

前記ライセンスを生成するライセンス生成ステップと、

前記ライセンスに、識別番号であるライセンスIDを付与するライセンスID付与ステップと、

前記ライセンスに、前記受信装置において、少なくとも当該ライセンスを当該受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限を付与するライセンス取り込み期限付与ステップと、

少なくとも前記ライセンスID、前記ライセンス取り込み期限が付与された前記ライセンスを、前記受信装置に送出する送出ステップと

をコンピュータに実行させることを特徴とするプログラム。

[32] ライセンスに基づきコンテンツを利用する端末装置と連携して動作するセキュリティモジュールに用いるプログラムであって、

前記ライセンスには、少なくとも前記ライセンスを前記受信装置に取り込み、利用可能な状態とする期限であるライセンス取り込み期限及びライセンスIDが付与され、

前記プログラムは、

前記送出装置から送出される前記ライセンスを取り込むライセンス取り込みステップと、

少なくとも前記ライセンス取り込み期限まで、前記ライセンスIDと前記ライセンス取り込み期限とを含むライセンス取り込み履歴を記録する履歴記録ステップと、

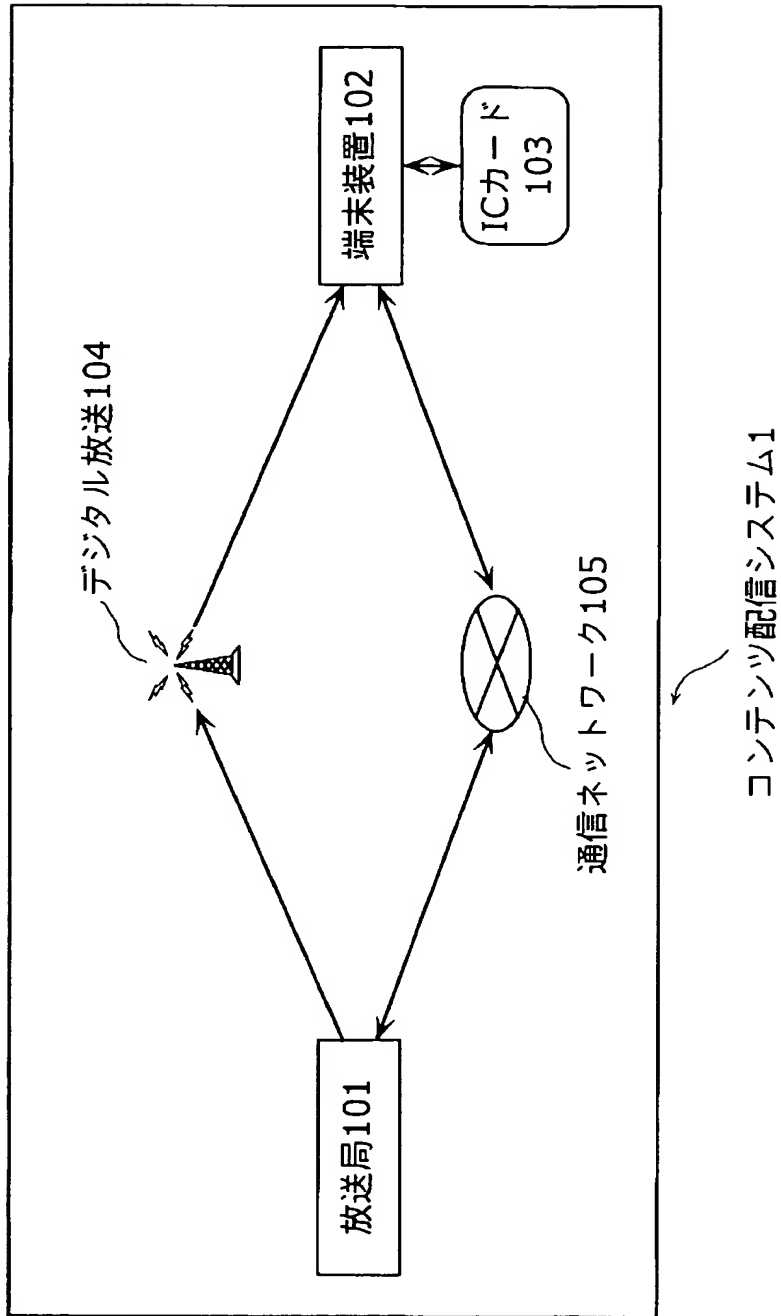
前記ライセンス取り込みステップにおいて取り込んだライセンスのライセンスIDと同一のライセンスIDが前記ライセンス取り込み履歴に存在する場合に、前記ライセンス取り込みステップにおける当該ライセンスの取り込みを抑制するライセンス取り込み抑制ステップと

をコンピュータに実行させることを特徴とするプログラム。

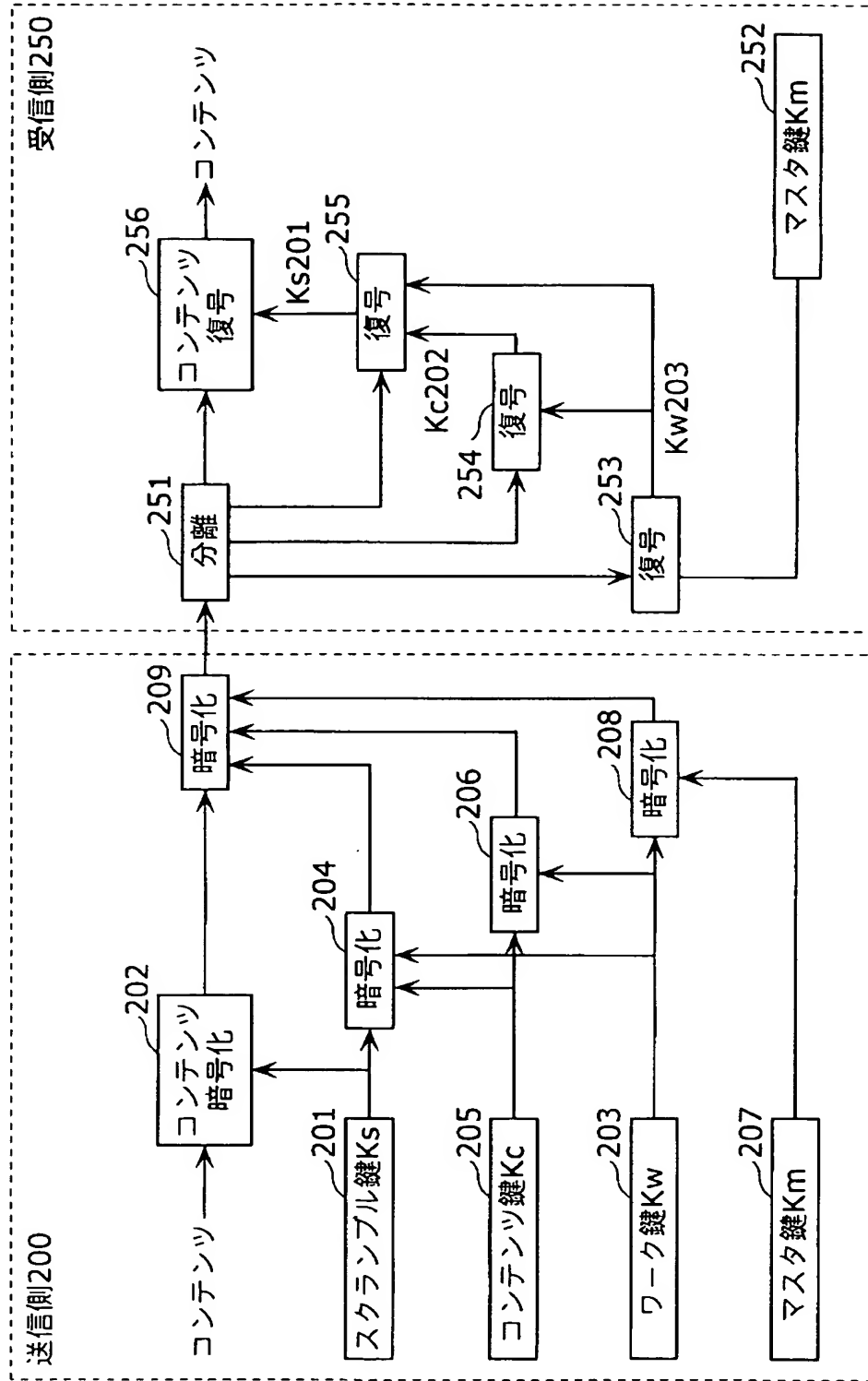
要 約 書

デジタル放送で配信するライセンスの不正取得を抑制し、事業者の権利を保護可能なデジタル権利管理システムを提供するために、送出装置である放送局は、生成するライセンスにIDとライセンス変換期限を付与し端末装置102に送信する。端末装置102は、ライセンスに付加されたライセンスIDとライセンス変換期限とを含むライセンス取得履歴を記録する。また、端末装置102は、ライセンスの取得時に既に同一ライセンスを取得している場合は、ライセンスの取得を抑制する。また、端末装置102が受信したライセンスは少なくともライセンス変換期限まで保持される。

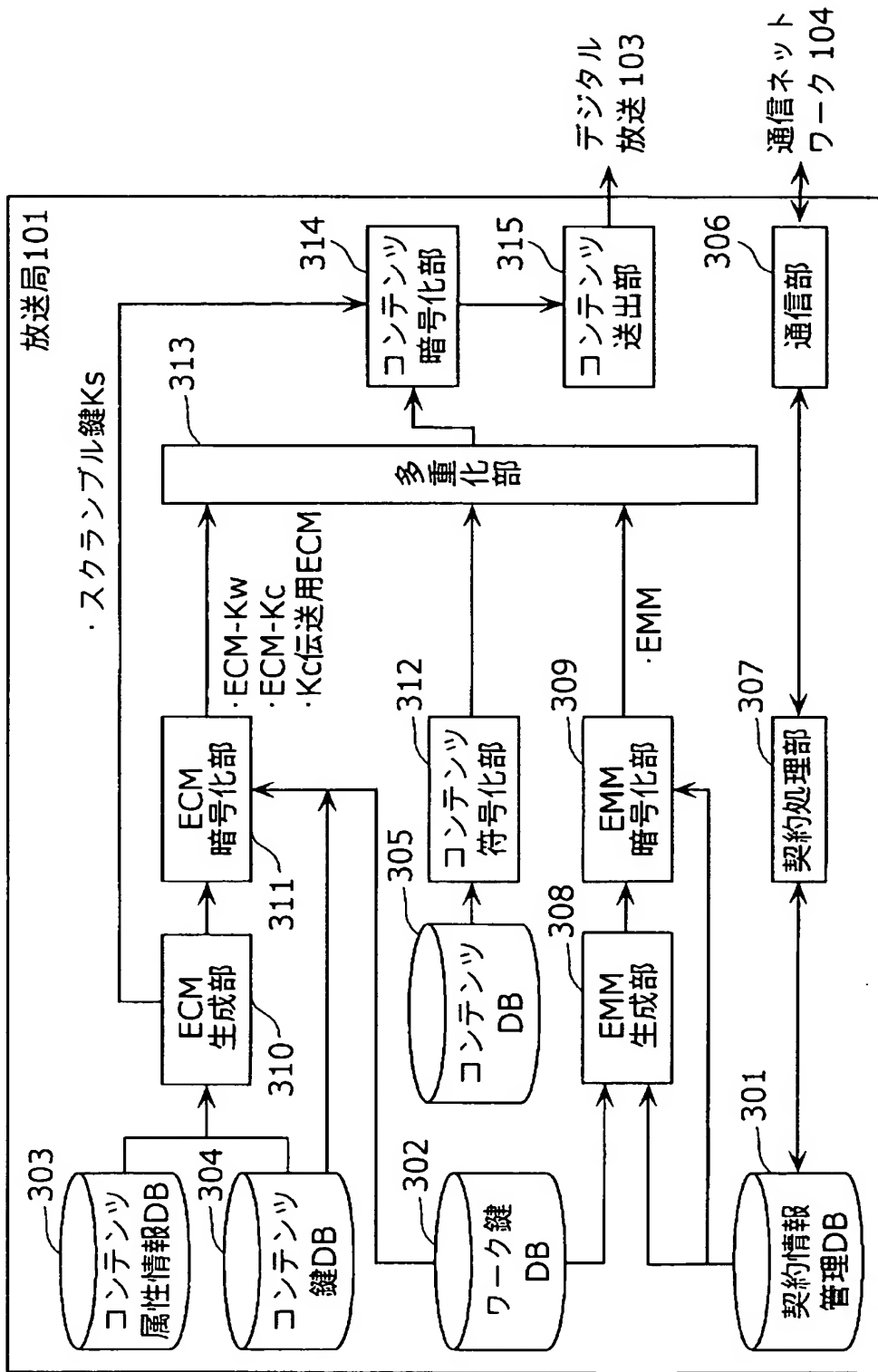
[図1]



[図2]



[図3]



[図4]

カードID	ティア契約ID	PPV契約ID	有効期限	蓄積暗号鍵Km'	マスク鍵Km
CARD-ID-1	TIERCONT-ID-1	PPVCONT-ID-1	2004/4/1~ 2005/3/31	0x111...111	0x111...111
CARD-ID-2	TIERCONT-ID-1	PPVCONT-ID-2	2003/12/1~ 2004/11/30	0x222...222	0x222...222
CARD-ID-3	TIERCONT-ID-2	PPVCONT-ID-1	2004/1/1~ 2004/4/30	0x333...333	0x333...333
CARD-ID-4	TIERCONT-ID-3	PPVCONT-ID-1	2004/1/1~ 2005/3/31	0x444...444	0x444...444
...

契約情報管理テーブル400

[図5]

ワーク鍵ID	ワーク鍵Kw	ワーク鍵利用開始日
WK-ID-1	0x123...cdf	2003/11/24
WK-ID-2	0x001...999	2004/12/20
...

ワーク鍵管理テーブル500

[図6]

601 コンテンツID	602 ライセンスID	603 利用条件	604 契約情報	605 ライセンス 変換期限
CONTENT-ID-1	LICENSE-ID-1	有効期間:1ヶ月	TIERCONT-ID-1	2004/4/30
CONTENT-ID-2	LICENSE-ID-2	有効期間:1ヶ月、再生回数:10回	TIERCONT-ID-1 TIERCONT-ID-2	2004/4/15
CONTENT-ID-3	LICENSE-ID-3	有効期間:3ヶ月	TIERCONT-ID-1	2004/4/25
CONTENT-ID-4	LICENSE-ID-4	有効期間:3日、書き出し回数:1回	PPVCONT-ID-1	2004/5/1
...

コンテンツ属性情報管理テーブル600

[図7]

701 コンテンツID	702 ライセンスID	703 コンテンツ鍵Kc
CONTENT-ID-1	LICENSE-ID-1	0x123...cdf
CONTENT-ID-2	LICENSE-ID-2	0x001...999
CONTENT-ID-3	LICENSE-ID-3	0xabc...def
CONTENT-ID-4	LICENSE-ID-4	0x123...123
...

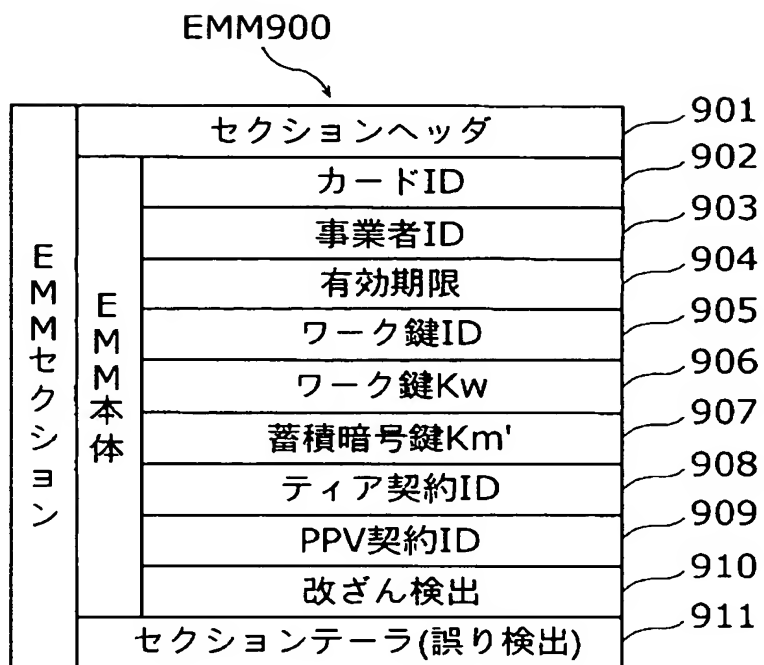
コンテンツ鍵管理テーブル700

[図8]

801	802	803	804
コンテンツID	コンテンツ名称	放送時間	ファイル名
CONTENT-ID-1	マンデースポーツ	2004/4/8 21:00:00	/SPORT/.../MONSPORTS.VC
CONTENT-ID-2	GOODBYE13	2004/4/8 22:00:00	/DRAMA/.../GOODBYE.VC
CONTENT-ID-3	網場の犬	2004/4/10 17:30:00	/ANIME/.../AMIBA.VC
CONTENT-ID-4	神器2	2004/5/1 19:00:00	/MOVIE/.../JINGI2.VC
...

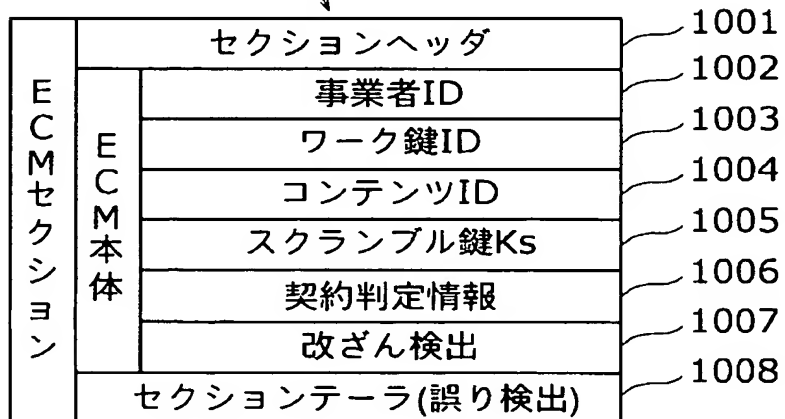
コンテンツ管理テーブル800

[図9]

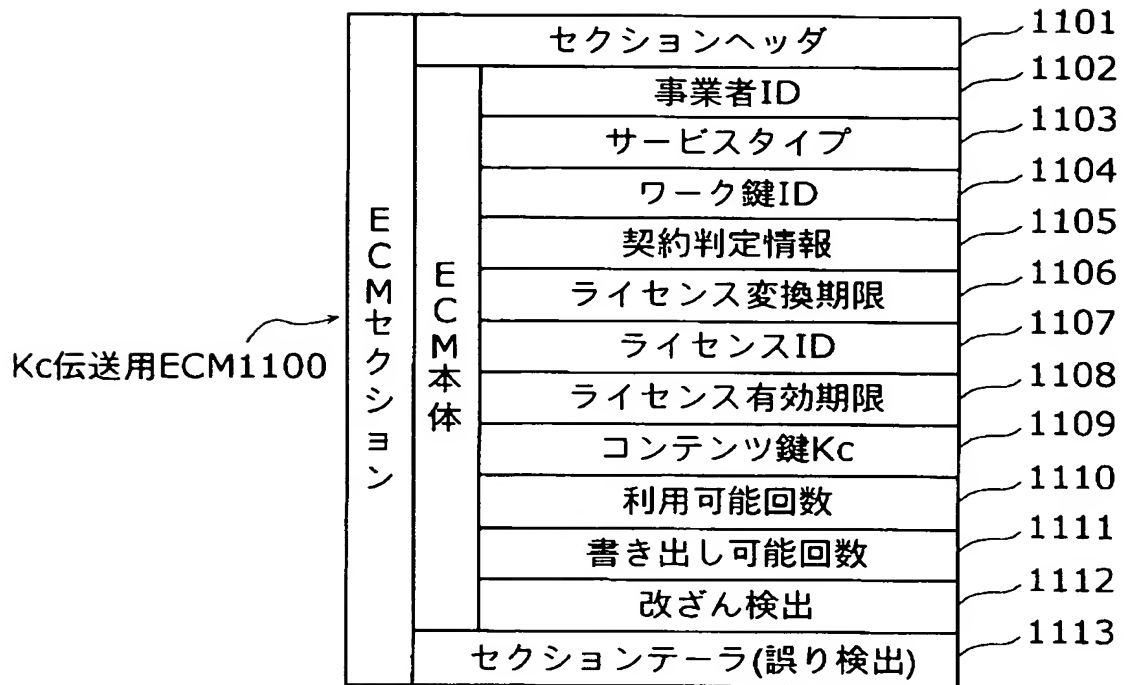


[図10]

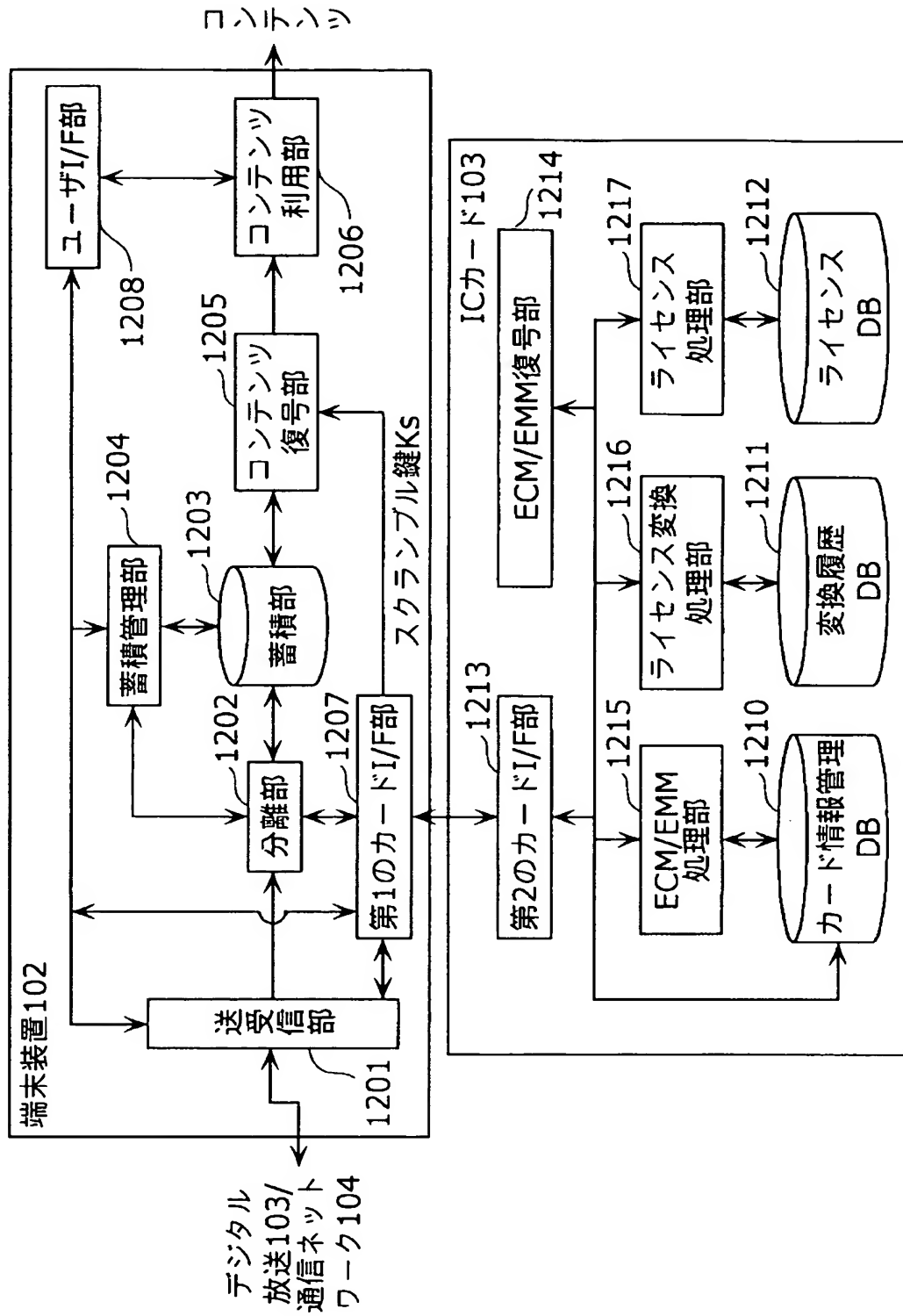
ECM-Kw1000、ECM-Kc1020



[図11]



[図12]



[図13]

1301	1302	1303
カードID	マスタ鍵Km	蓄積暗号鍵Km'
0x000・・・001	0x111・・・111	0x777・・・777

共通情報テーブル1300

[図14]

1401 事業者ID	1402 ティア契約ID	1403 PPV契約ID	1404 有効期限	1405 ワーク鍵ID	1406 ワーク鍵KW
SERVICE-ID-1	TIERCONT-ID-1	PPVCONT-ID-1	2004/4/1~ 2005/3/31	KW-ID-1	0x111...111
SERVICE-ID-10	—	PPVCONT-ID-1	2004/1/1~ 2005/3/31	KW-ID-1	0x555...555
...

事業者別情報テーブル1400

[図15]

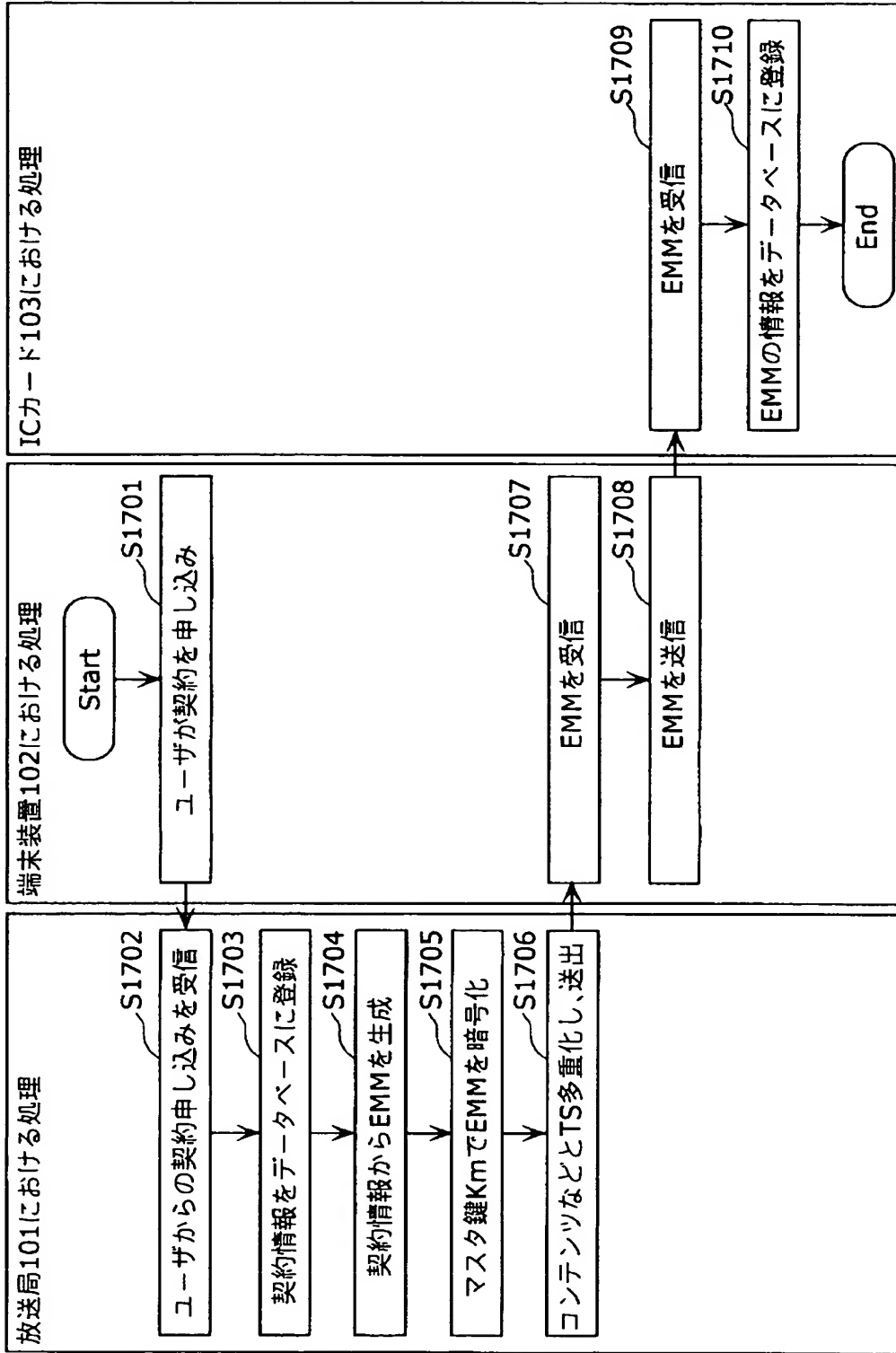
1501 ライセンスID	1502 ライセンス変換期限
LICENSE-ID-1	2004/4/30
LICENSE-ID-2	2004/4/15
LICENSE-ID-3	2004/4/25
LICENSE-ID-4	2004/5/1
...	...

TL1500

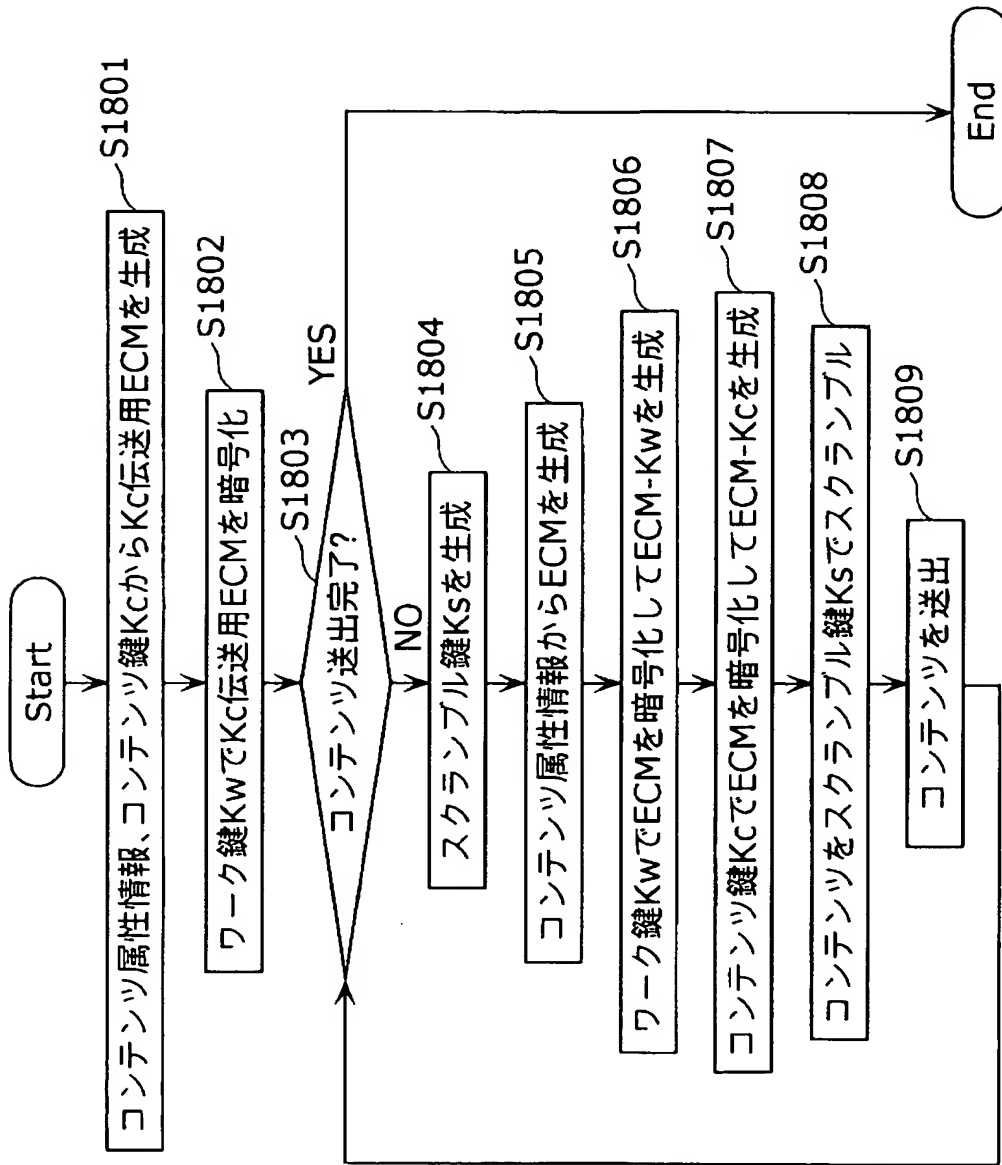
[図16]

ライセンス1600	
ライセンス識別子	1601
ライセンスID	1602
有効期限	1603
再生回数	1604
書き出し回数	1605
コンテンツ鍵Kc	1606
改ざん検出	1607

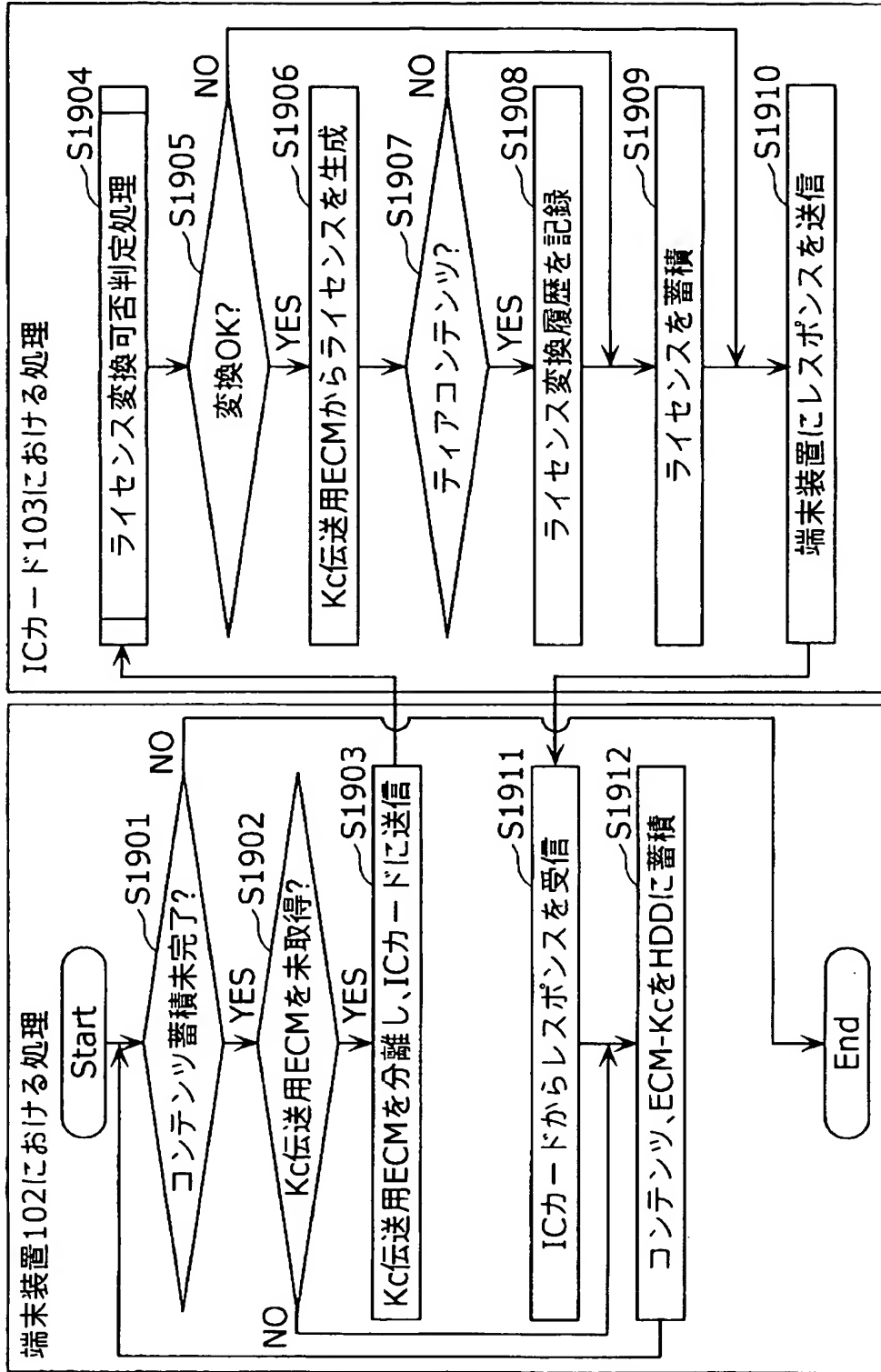
[図17]



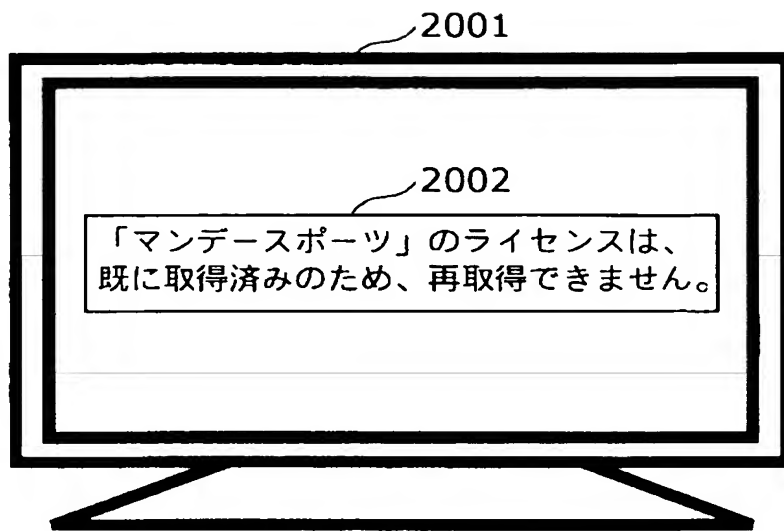
[図18]



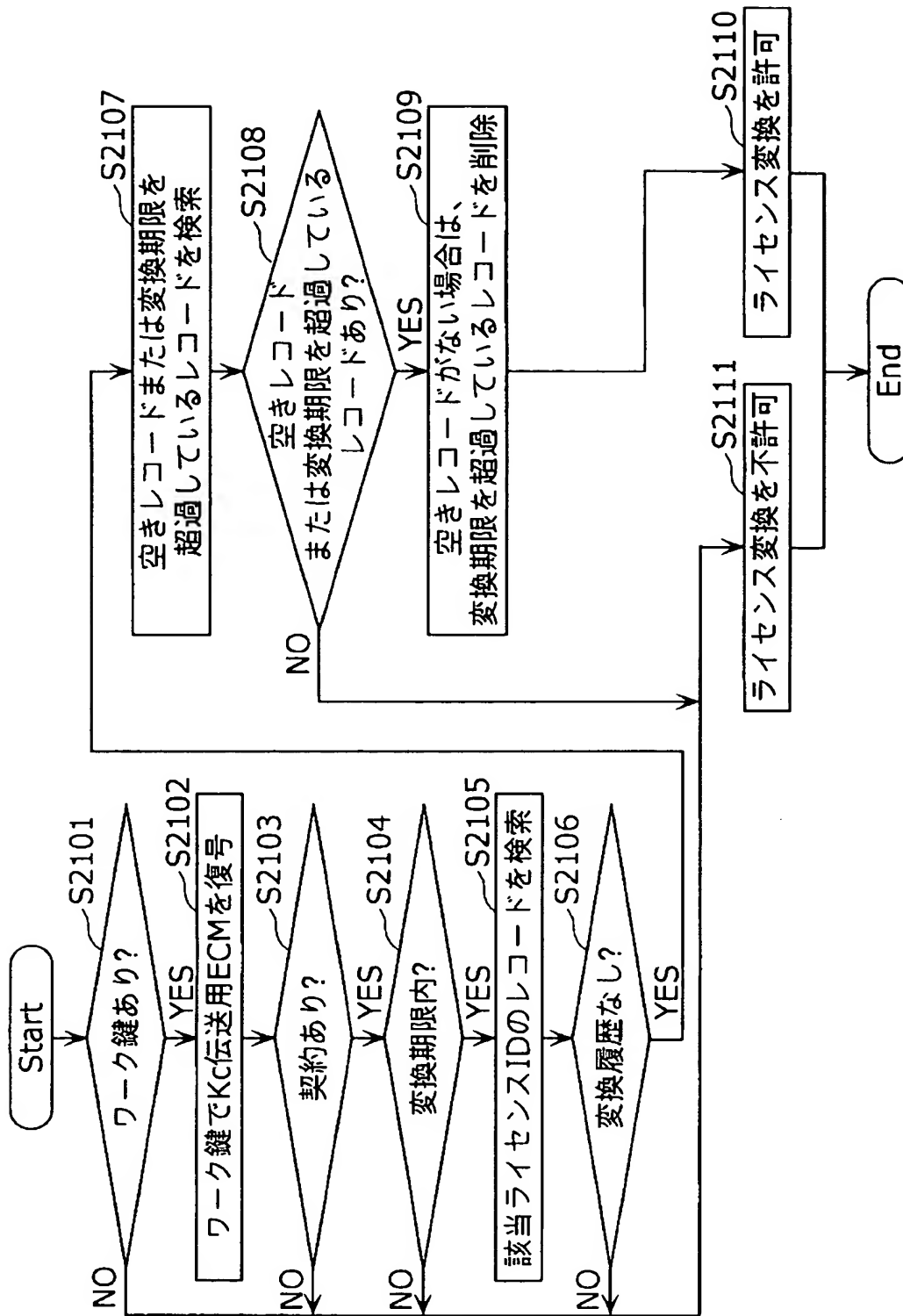
[図19]



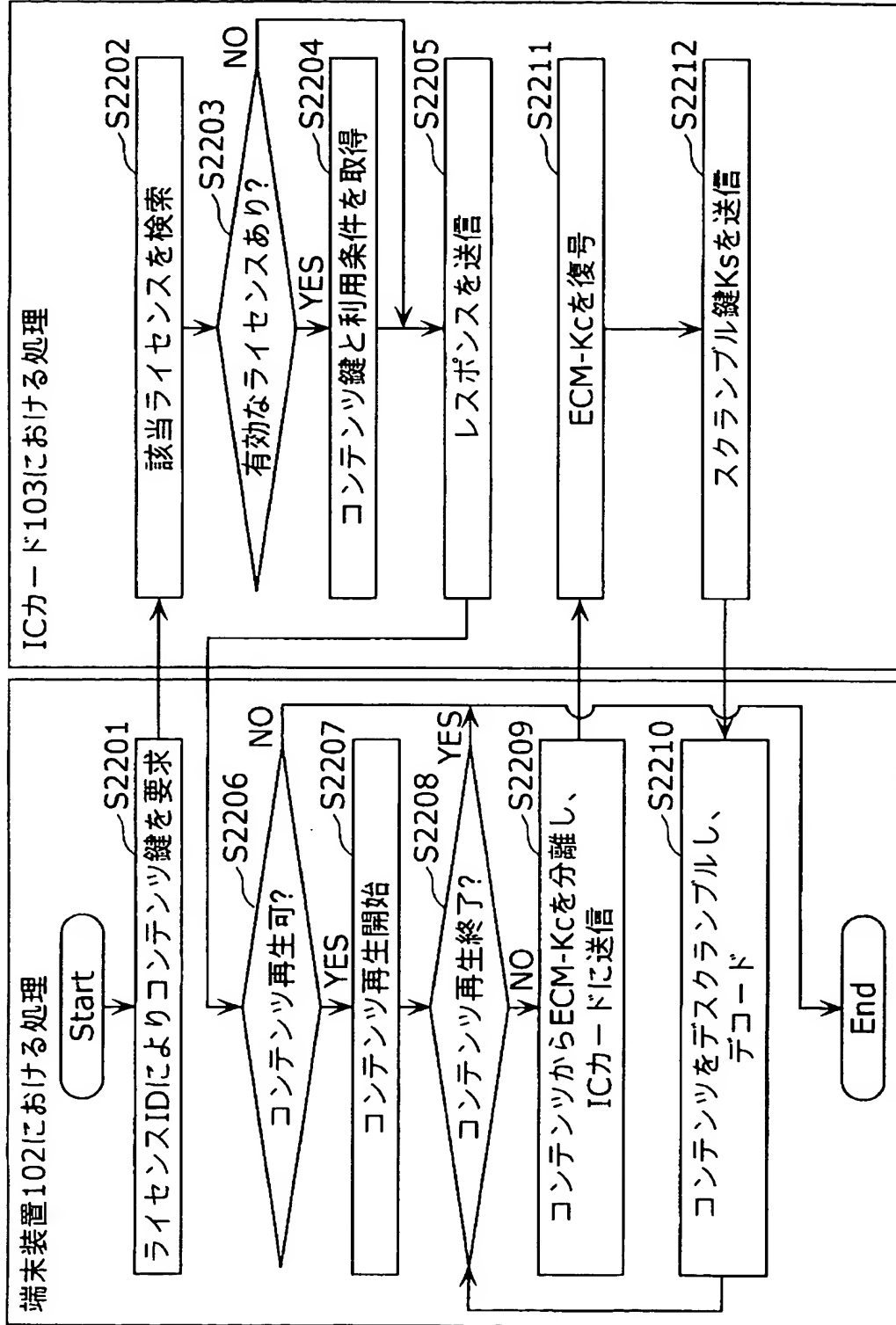
[図20]



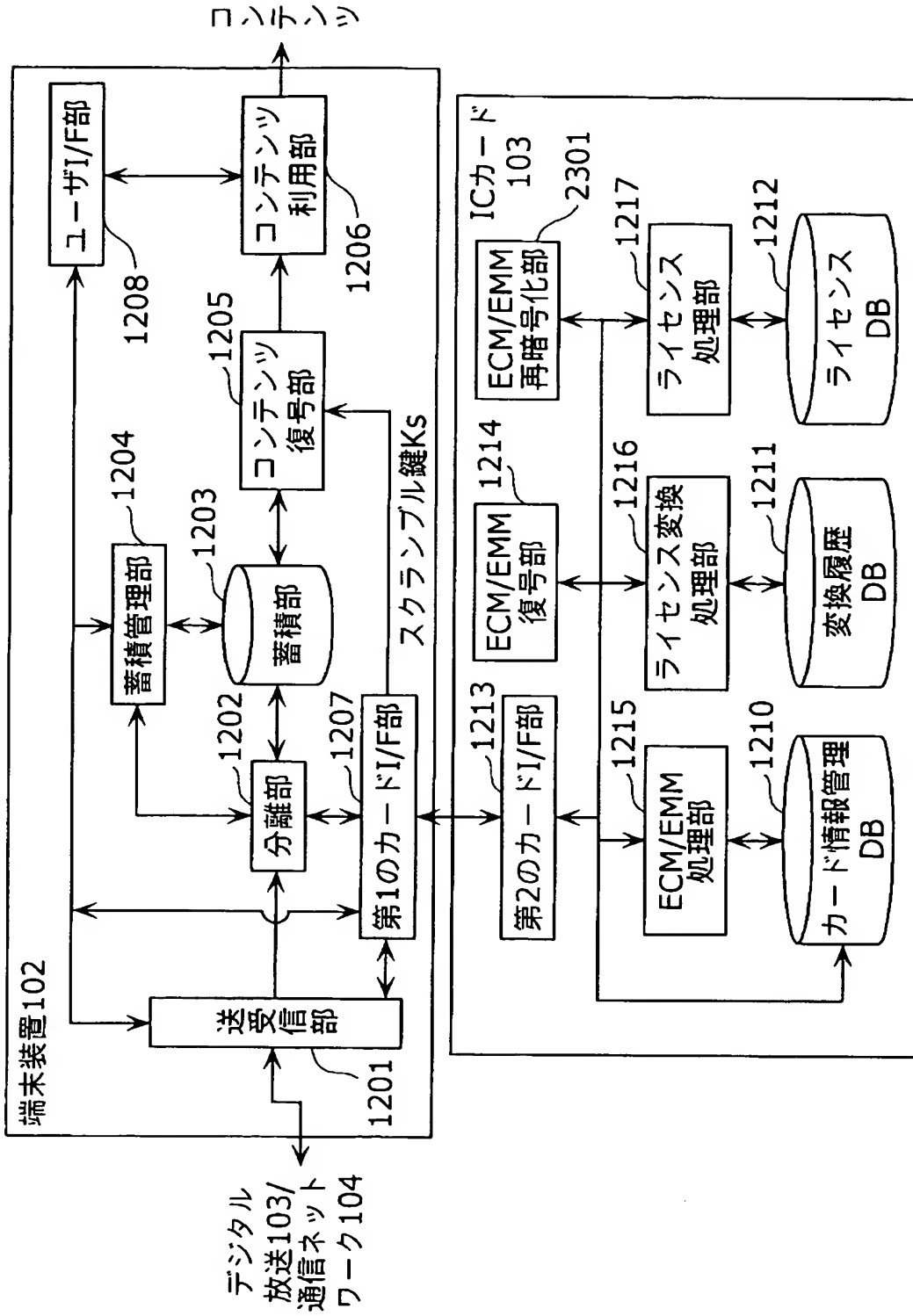
[図21]



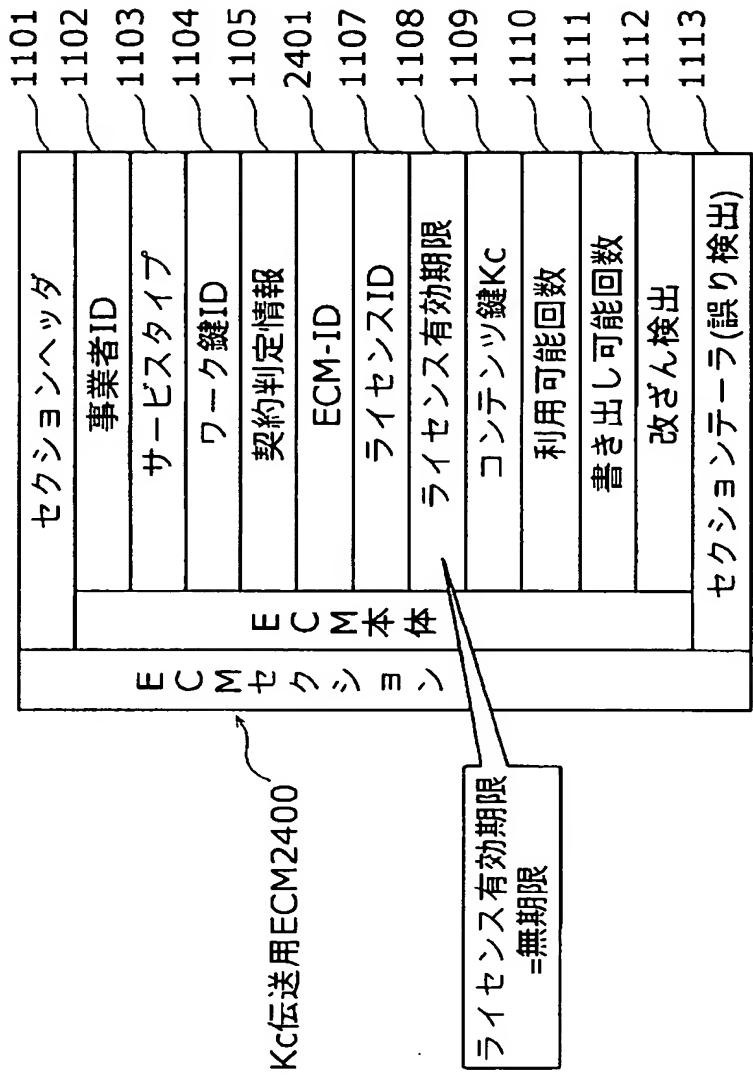
[図22]



[図23]



[図24]

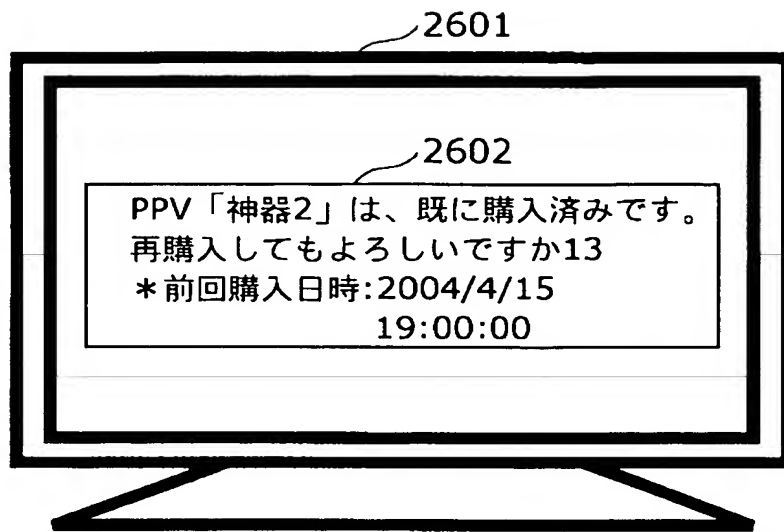


[図25]

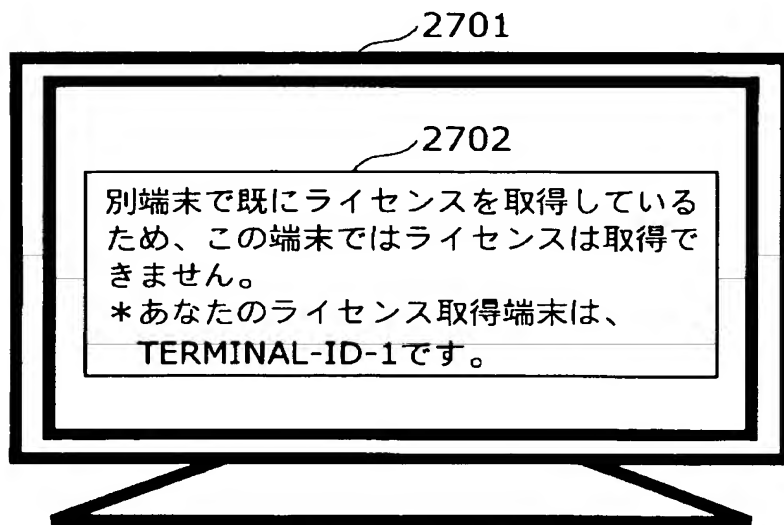
2501 事業者ID	2502 ライセンスID	2503 サービスタイプ	2504 購入情報	2505 ライセンス変換 期限	2506 取得ライセンス 数
SERVICE-ID-1	LICENSE-ID-1	TIERCONT	—	2004/4/15	2回/3回 (2004/4/14、 2004/4/15)
SERVICE-ID-5	LICENSE-ID-2	TIERCONT	—		
SERVICE-ID-30	LICENSE-ID-3	TIERCONT	—	2004/5/15	
SERVICE-ID-2	LICENSE-ID-4	PPVCONT	購入済み (2004/4/25)		1回/1回 (2004/4/24)
...

TL2500

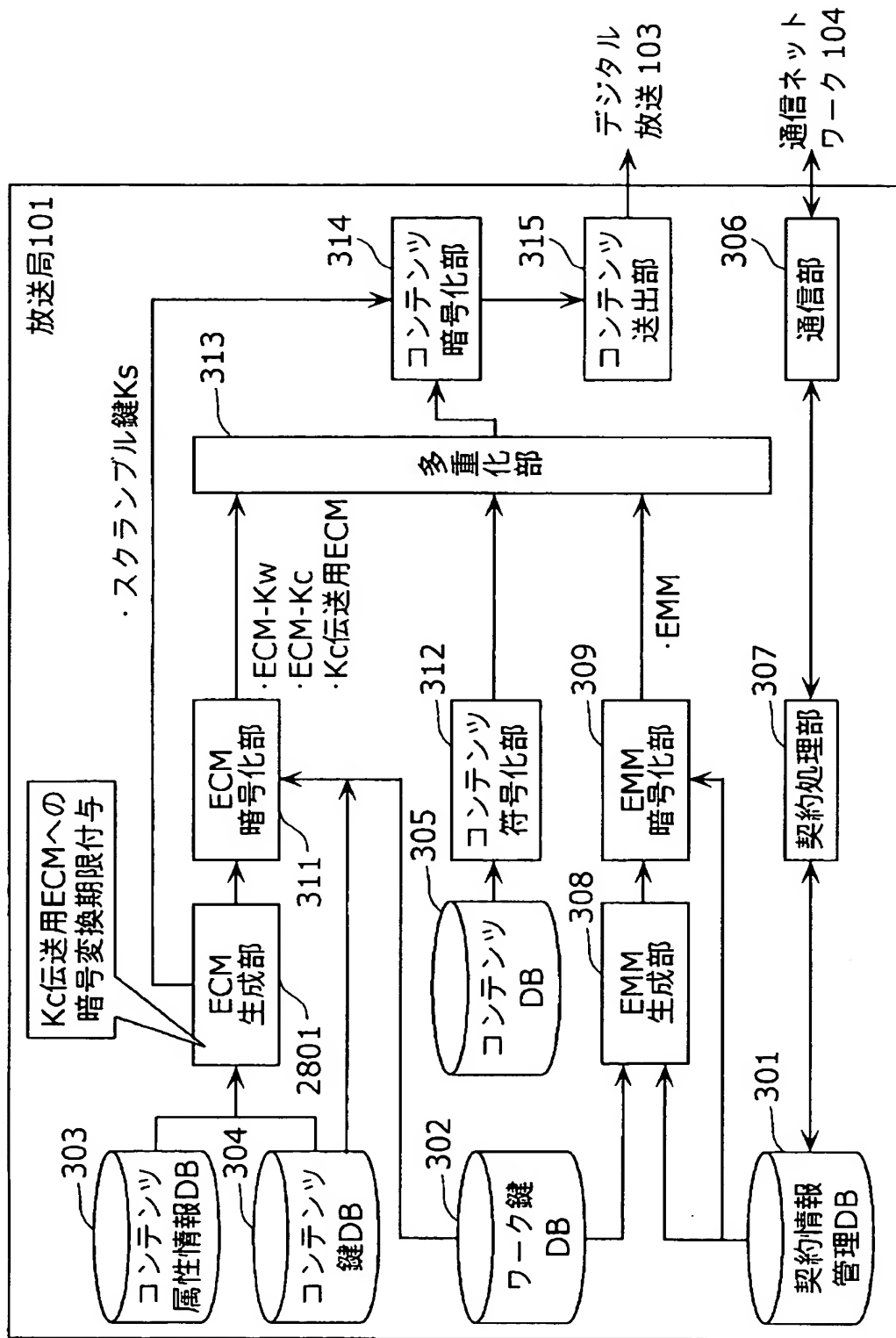
[図26]



[図27]



[図28]



[図29]

2901	2902	2903	2904	2905
コンテンツID	ライセンスID	利用条件	契約情報	暗号変換期限
CONTENT-ID-1	LICENSE-ID-1	有効期間:1ヶ月	TIERCONT-ID-1	2004/4/15
CONTENT-ID-2	LICENSE-ID-2	有効期間:1ヶ月、再生回数:10回	TIERCONT-ID-1 TIERCONT-ID-2	2004/4/18
CONTENT-ID-3	LICENSE-ID-3	有効期間:3ヶ月	TIERCONT-ID-1	2004/4/17
CONTENT-ID-4	LICENSE-ID-4	有効期間:3日、書き出し回数:1回	PPVCONT-ID-1	2004/5/14
...

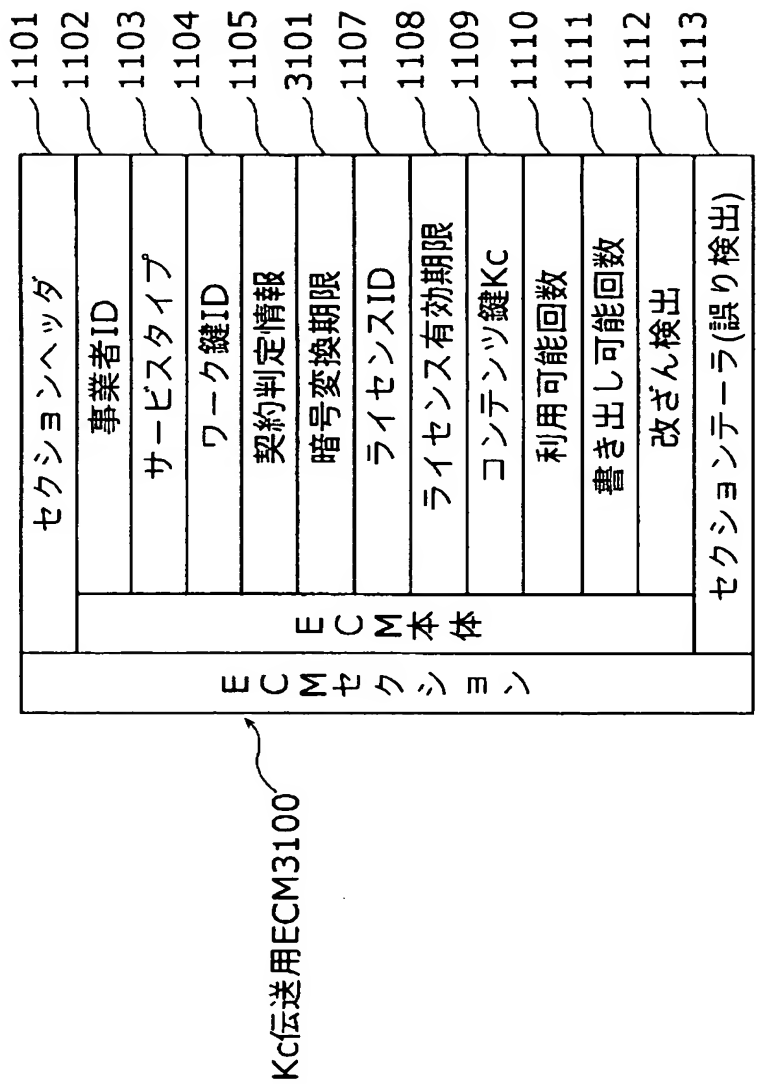
コンテンツ属性情報管理テーブル2900

[図30]

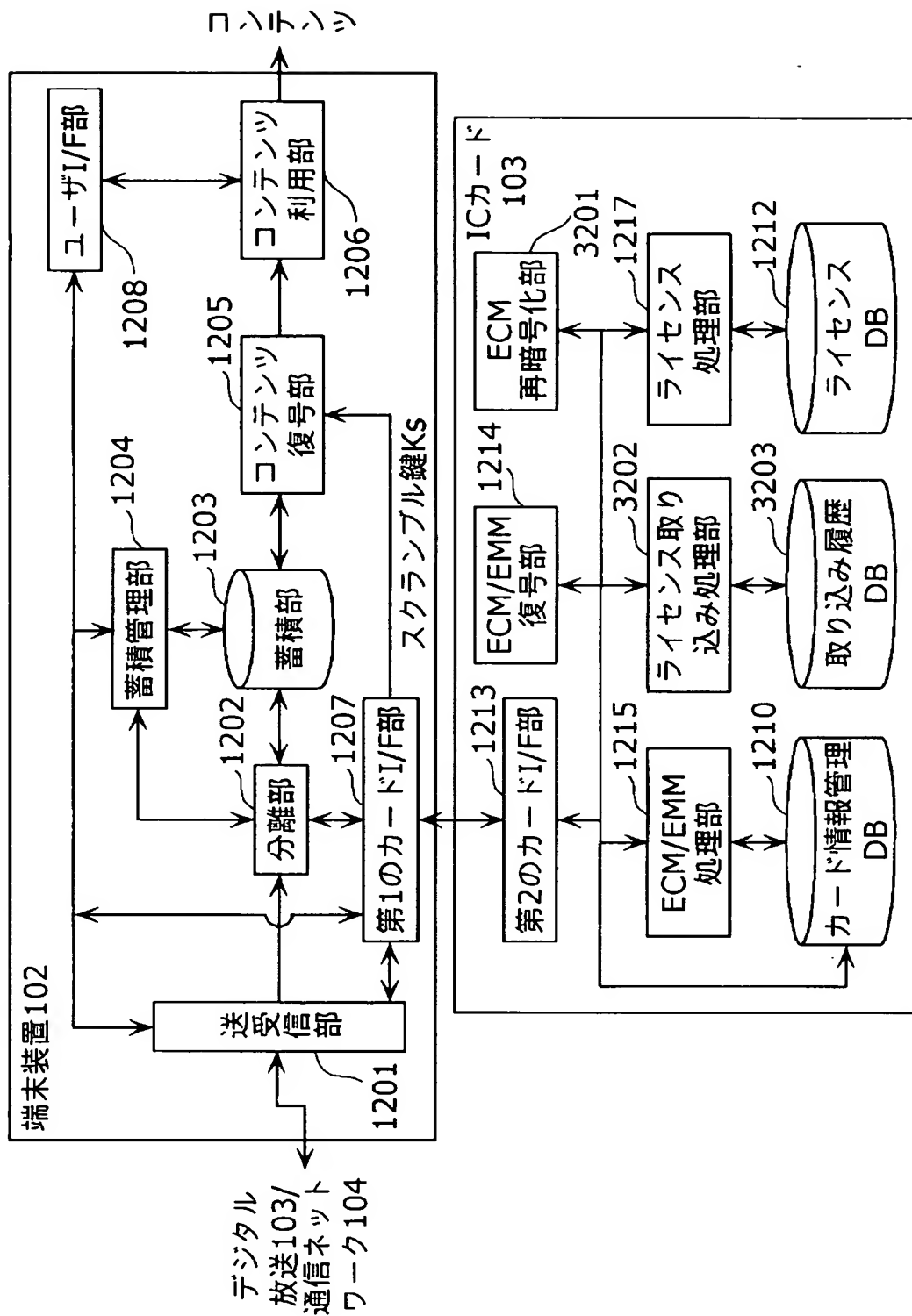
コンテンツID	コンテンツ名称	放送時間	ファイル名
CONTENT-ID-1	マンデースポーツ	2004/4/8 21:00:00	/SPORT/...MONSPORTS.VC
CONTENT-ID-2	GOODBYE13	2004/4/8 22:00:00	/DRAMA/...GOODBYE.VC
CONTENT-ID-3	網場の犬	2004/4/10 17:30:00	/ANIME/...AMIBA.VC
CONTENT-ID-4	神器2	2004/5/1 19:00:00	/MOVIE/...JINGI2.VC
...

コンテンツ管理テーブル3000

[図31]



[図32]

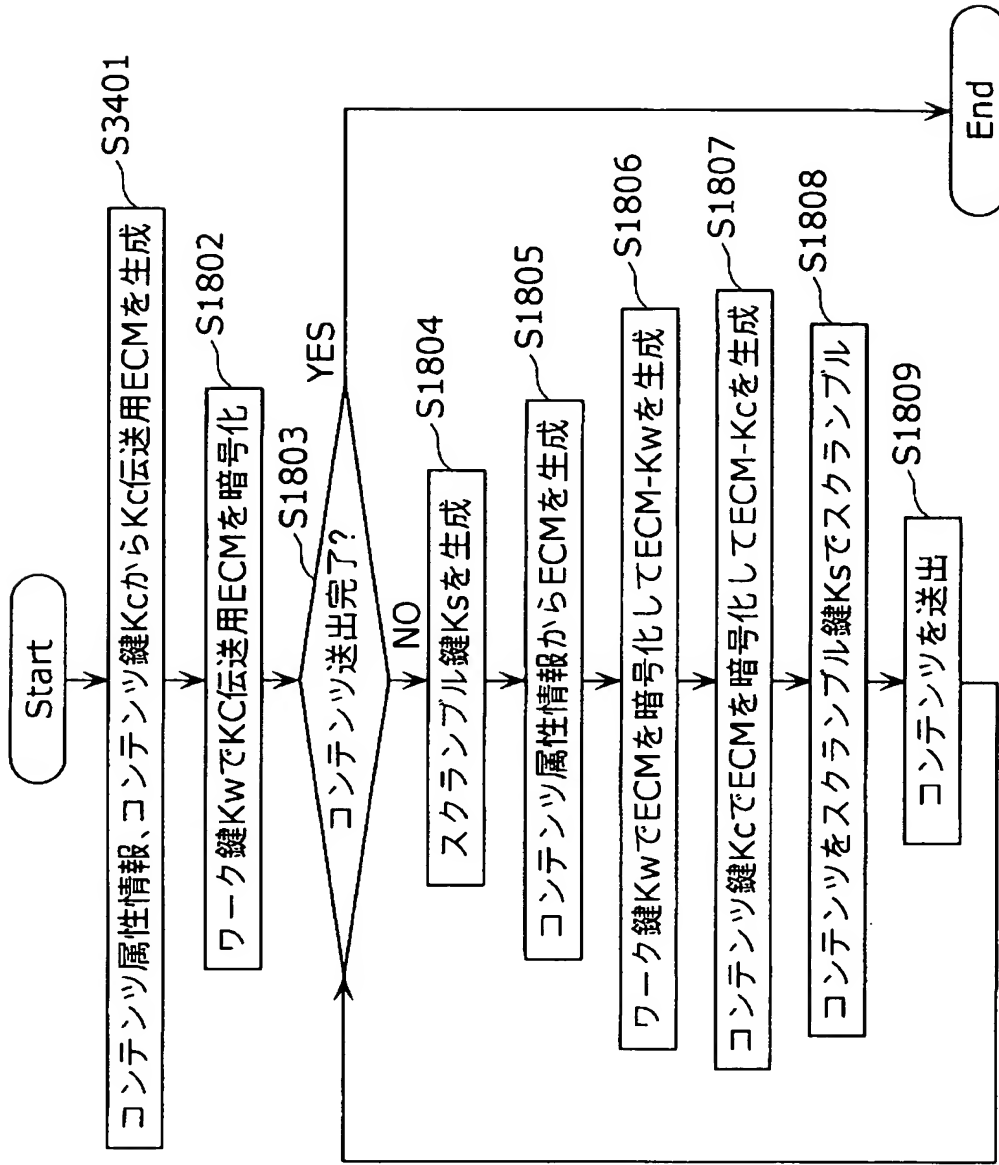


[図33]

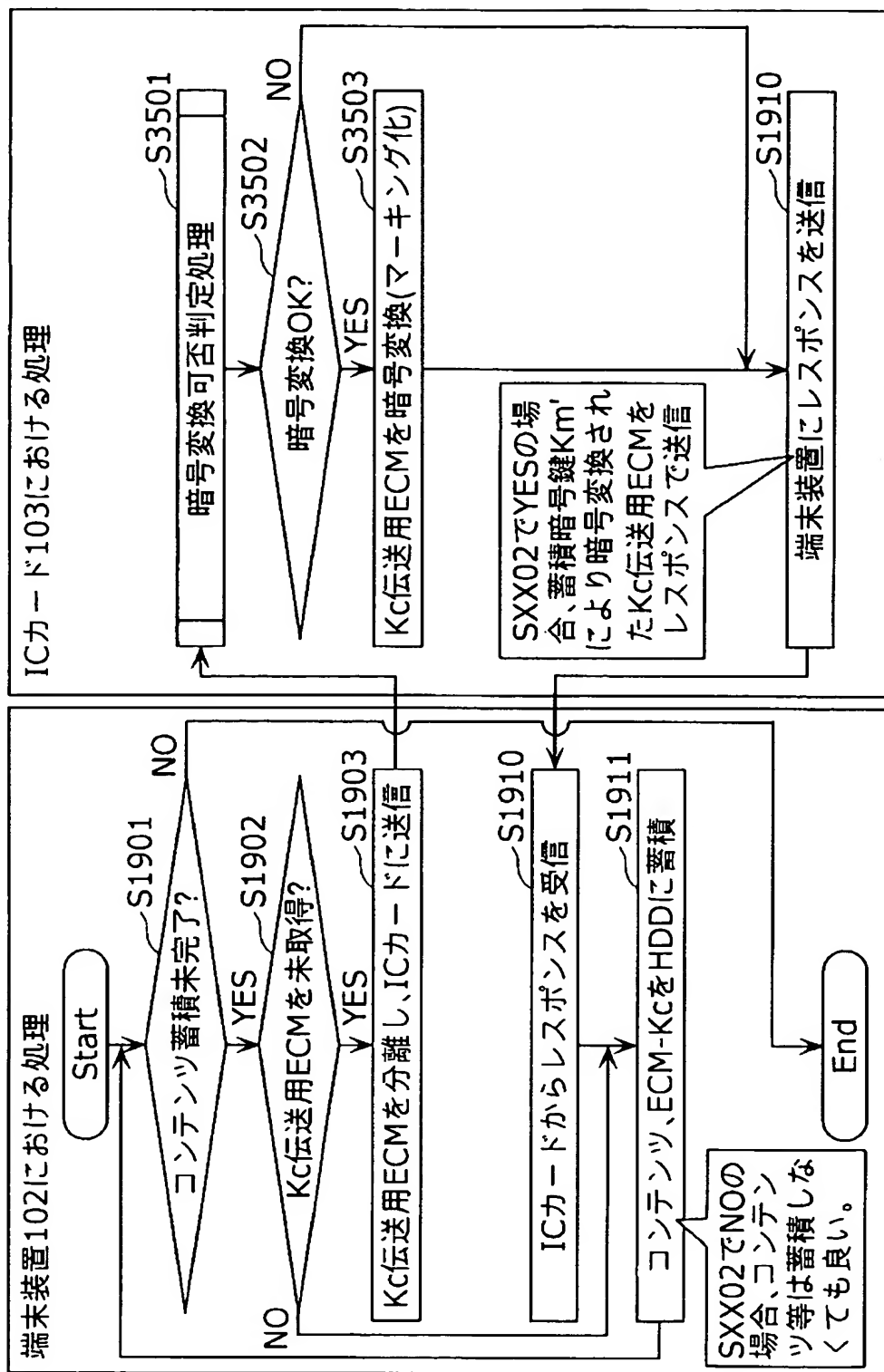
3301 ライセンスID	3302 ライセンスの有効期限
LICENSE-ID-1	2004/5/8
LICENSE-ID-2	2004/5/8
LICENSE-ID-3	2004/7/10
LICENSE-ID-4	2004/5/4
...	...

取り込み履歴テーブル3300

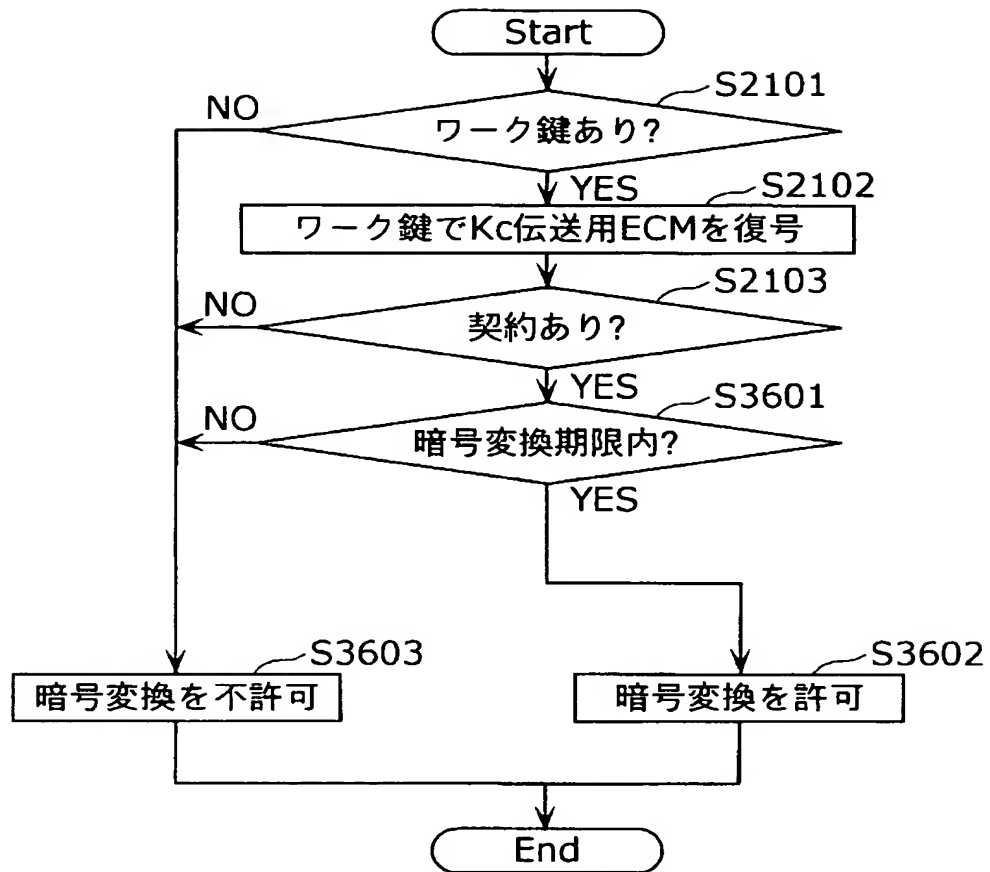
[図34]



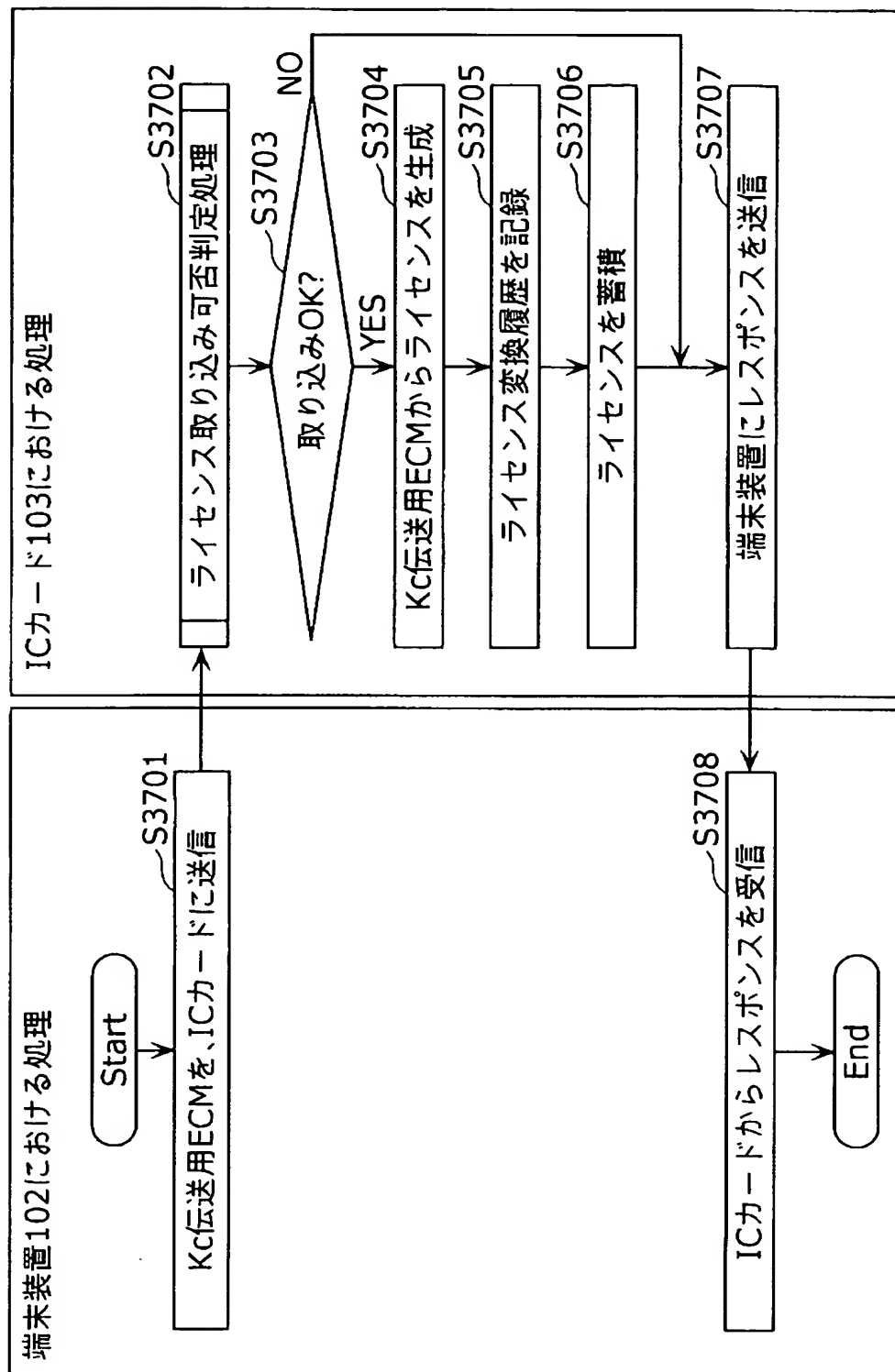
[図35]



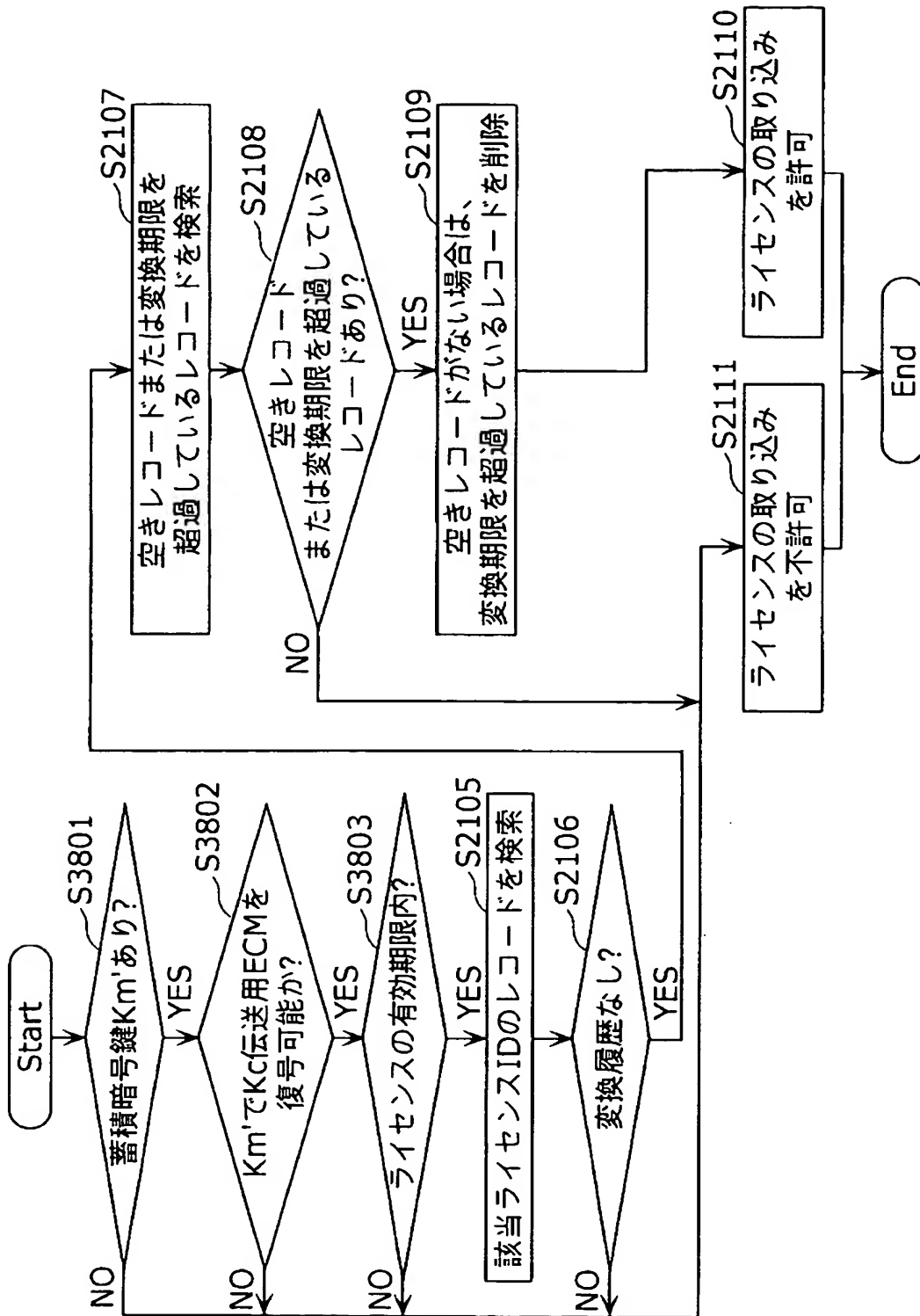
[図36]



[図37]



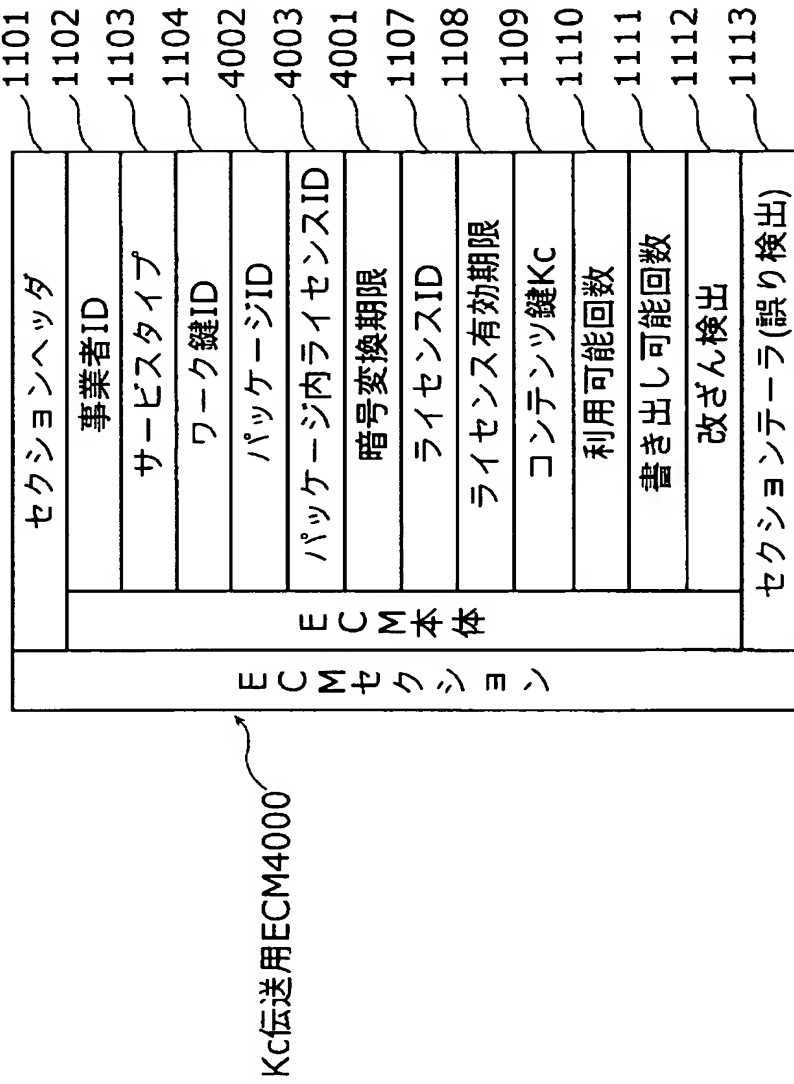
[図38]



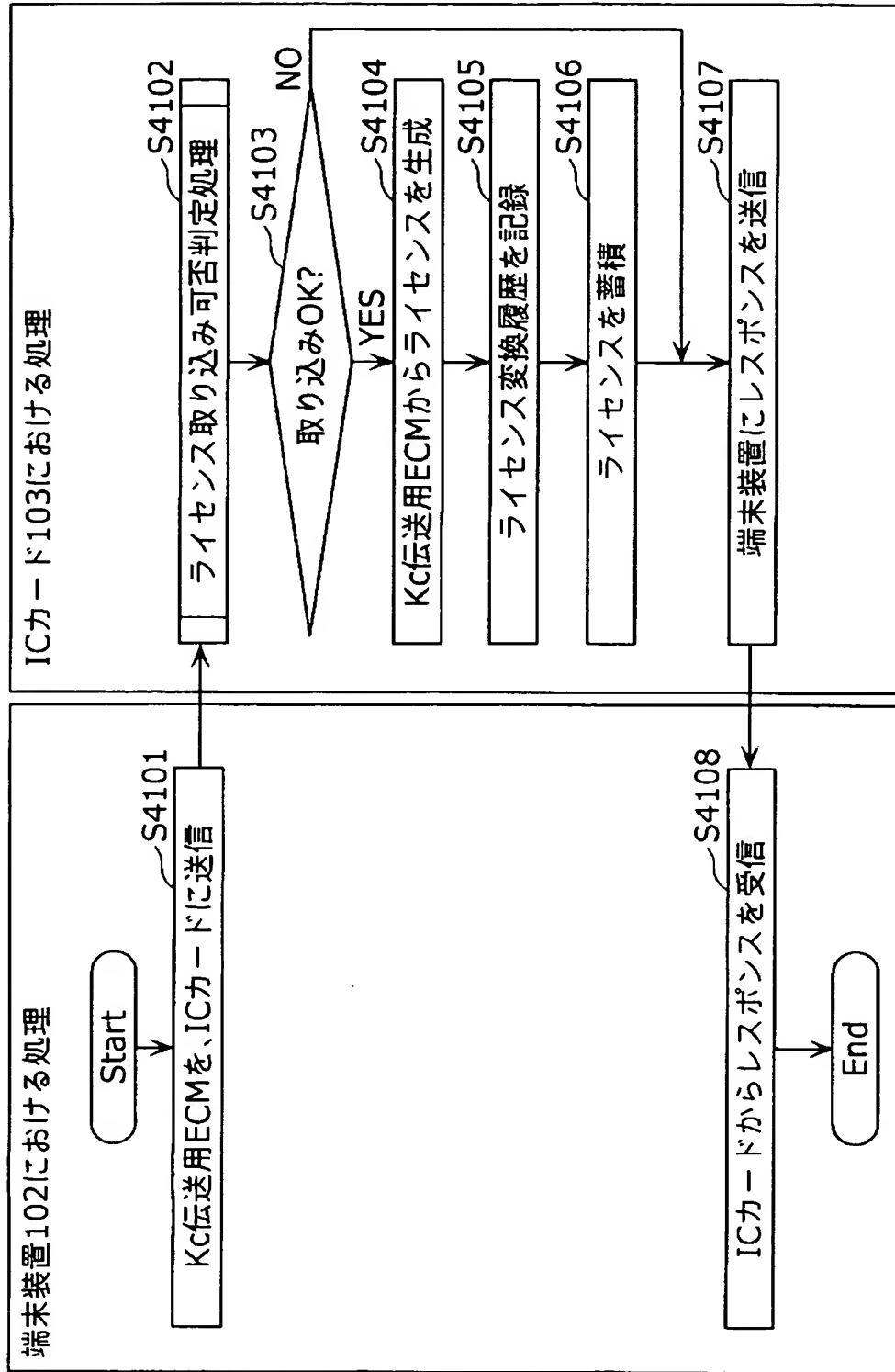
3901 パッケージID	3902 有効期限	3903 パッケージ内ライセンスID	3904 取得済みライセンスID
PKG-ID-1	2004/5/8	LICENSE-ID-1 LICENSE-ID-2 ... LICENSE-ID-10	LICENSE-ID-1 LICENSE-ID-2
PKG-ID-2	2004/5/8	LICENSE-ID-100 LICENSE-ID-101	LICENSE-ID-101
...

取り込み履歴テーブル(IL:Import List)3900

[図40]



[図41]



[図42]

